International Institute of Information Technology

Hyderabad

System and Network Security (CS5470)

Assignment 4

Total Marks: 100 [Implementation (Coding + correct results): 60, quiz: 40]

Instructions:

1. Submit your solution in an zip file. The archive should be named lab_assignment4.zip.
2. The archive should contain a directory for every question. The directory should be named question<question-number>.
3. Each directory should contain a file named input.txt and a directory named screenshots.
4. The directory screenshots should contain screenshots of successful exploits for all the questions.

1.Create an environment variable **MALICIOUS**, such that when it is read into the buffer, it overflows the buffer in a manner which prints “updateMe successfully updated!”

- The goal of this exercise is to demonstrate that vulnerabilities can be exploited not just from interactive user input, but from other avenues of input like environment variables too.
- Additionally, to check if a software is vulnerable or not, data should be crammed into every type of input like environment variables, command line input, network input, GUI fields, menus etc.
- Submit your input in the answer file.
- Submit a screenshot of successful exploit.

Marks-15

2.Provide input to the program such that the function **executeme** is executed.

- You will need to overwrite the **functionPointer** function pointer.
- The goal of this exercise is to teach you function pointer overwrite attack. This attack was to be covered in the next tutorial, but then I trust that all of you can do it yourself.
- Submit your input in the answer file.
- Submit a screenshot of successful exploit.

Marks-10

3.Provide input to the program such that the function **executeme** is executed.

- The goal of this exercise is to demonstrate that a suitably crafted input can modify the normal execution flow of the program
- Submit your input in the answer file.
- Submit a screenshot of successful exploit.

Marks-10

.

4.Provide input to the program such that it prints

“**Updatedsuccessfully**!”

- The goal of this exercise is to teach you to craft your input in such a manner such that it overwrites a specific address space with a specific value.
- Submit your input in the answer file.
- Submit a screenshot of successful exploit.

Marks-10

5.Provide input to the program such that it overwrites **updateMe** variable.

- The goal of this exercise is to demonstrate that a buffer overflow can modify
- The address space located before the vulnerable overflowed buffer.
- Submit your input in the answer file.
- Submit a screenshot of successful exploit.

Marks-15

For Quiz purpose and assignment purpose..(read)
http://insecure.org/stf/smashstack.html
For return-to-libc-attack-(quiz)
https://www.youtube.com/watch?v=pVBnjSQ4Fjk
https://www.youtube.com/watch?v=GwtPmwa2PLg

Write proper reason for each and every step you will do and also provide screenshot of each step.