CISC 367 – Spring 2016

Homework Assignment – Buffer Overflow Attack on Raspberry Pi

In this assignment, you will learn how to exploit buffer overflow vulnerability on the ARM platform. You should study the ARM architecture by watching the following video

- The ARM University Program, ARM Architecture Fundamentals

and reviewing the following documents.

- Practical ARM Exploitation Lab Manual Preview
- Exploiting ARM Linux Systems An introduction

You will be running the Raspbian operating systems on Raspberry Pi. The key is to figure out the equivalents of `$rbp` and `$rsp` in the ARM architecture, respectively.

Again, exploit the same `test.c` and `jumpover.c` programs.

1. Given C program `test.c`, produce an input string, via the help of `gdb`, that will trigger function `bar()` to be invoked and message "Why am I here???" printed.

   Use Unix command `script` to capture the execution trace of running `test.c` with your produced string as the command-line argument (in terms of a Python expression).

   In addition to submitting a Python expression, you should also describe how you come to this Python expression. You may use "script" to capture the `gdb` session you use to derive the answer.

2. Given C program `jumpover.c`, use `gdb` to figure out the (integer) values needed in lines 7 and 8, respectively, so that the message "`this line should not be printed...`" will not be printed.