NUS CS-3235: Computer Security October 22, 2020

Assignment 2 Report - Part 2

Lecturer: Reza Shokri *Student: Wang Xinman A0180257E*

1 Format String

1.1 Running exploit

./format_string < payload

1.2 Methodology

1. Found addresses of jackpot with p &jackpot: 0x55555575501c
2. Attempted a sample input of "AAAAAAAA\x1c\x50\x75\x55\x55\x55\x00\x00"
   (a) Using GDB, it is found that the address supplied is the second entry on the stack, so it is the 7th argument from printf.
3. As such, %7 is used to point printf to the 7th argument. $n is used to write an arbitrary number of bytes to the address at the 7th argument.
4. However, as 4919 bytes are needed, %4919c is needed at the start of the payload to write 4919 (0x1337) to jackpot.
   (a) As %4919c is longer than 4 characters, it pushes the 7th argument back by 1, and so the address of jackpot supplied is now the 8th argument.
5. So the start of the payload has to be changed to %4919c%8$n.
6. A padding of "AAAAAA" is needed to align the payload to multiples of 8 bytes.

Running the command gives:

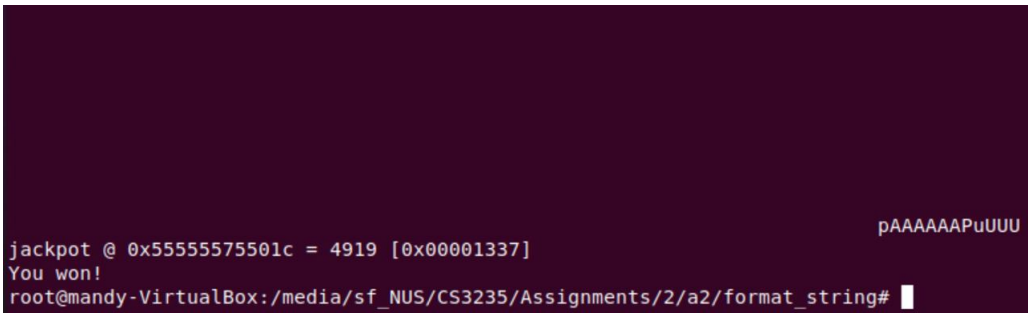

Figure 1: Working result