Dom Arishi

Lab7

2107

11/15/2020

1. **What is the command to compile the files with extra symbols that are useful for GDB?**

* **gcc -g GDBassign.c blowfish.c**

1. **What's the address of stuff?**

* **gdb a.out**
* **break GDBassign:381**
* **run**
* **print x stuff**
* **$1 = (uint32\_t (\*)[720]) 0x7fffffffc290**

1. **What's the address of stuff[0]?**

* **x &stuff[0]**
* **$2 = (uint32\_t \*) 0x7fffffffc290**

1. **we expect these to be the same? Why? Explain what the [ ] operator does in C?**

* **So we expect these to be the same because since the pointer to the entire array reference the 1st element of the array, so the [ ] operator adds subscript to base address of array and then get value on resulting address.**

1. **In Blowfish\_Init( ), what is the value of key?**

* key = **0x400ce0 "LAME\_KEY"**

1. **What command(s) did you type in order to learn this?**

* **break Blowfish\_Init**
* **run**
* **print key**

1. **In Blowfish\_Init( ), what are the values of i and j after the nested for loops have finished?**

**i.e., after:**

**for (i = 0; i < 4; i++) { for (j = 0; j < 256; j++)**

**ctx->S[i][j] = ORIG\_S[i][j]; }**

* **i = 4**
* **j = 256**

1. **What command(s) did you type in order to learn this?**

* **break Blowfish\_Init**
* **break 720**
* **continue**
* **p i**
* **p j**

1. **Before the Blowfish\_Encrypt function is called, what is the value of stuff[3] (for each, print the value, and the command used to obtain the value?**

**In Hex?**

* p /x stuff[3]

0x20656874

**In Binary?**

* p /t stuff[3]

100000011001010110100001110100

**As float?**

* p /f stuff[3]

1.94316151e-19

**As 4 chars?**

* x /4c &stuff[3]
* 0x7fffffffc29c: 116 't' 104 'h' 101 'e' 32 ' '

1. **Before the Blowfish\_Encrypt function is called, what is the value of stuff if we treat it as a string? (You don't have to write the whole string. Just describe what's there.) What was the command typed in order to obtain this value?**

* x /s stuff

1. **What is the value of x the first time that the function F() in Blowfish.c is called?**

* Breakpoint at blowfish.c:550
* run
* p x
* $1= 1753098189

1. **What is the output if we run GDB's backtrace (abbreviated "bt") command inside the function F() in Blowfish.c the first time F() is called? Briefly explain the output of the command in your own words?**

* (gdb) bt
* #0 F (ctx=0x7fffffffc7d0, x=1753098189) at blowfish.c:550
* #1 0x0000000000400749 in Blowfish\_Encrypt (ctx=0x7fffffffc7d0, xl=0x7fffffffc7a4, xr=0x7fffffffc7a0) at blowfish.c:602
* #2 0x0000000000400974 in Blowfish\_Init (ctx=0x7fffffffc7d0, key=0x400be0 "LAME\_KEY", keyLen=8) at blowfish.c:754
* #3 0x0000000000400581 in main () at GDBassign.c:228
* bt or Backtrace is the series of currently active function calls for the program. So, bt() is showing the functions that were to get me to my current frame. In this case, main called Blowfish\_Init, which called Blowfish\_Encrypt, which also called the func F().