Microsoft Windows [Version 10.0.19042.1165]

(c) Microsoft Corporation. All rights reserved.

D:\one drive\OneDrive\Desktop\12190094\Assignment 1\bomb001>bash

tshering@TD:/mnt/d/one drive/OneDrive/Desktop/12190094/Assignment 1/bomb001$ gdb bomb

GNU gdb (Ubuntu 8.1.1-0ubuntu1) 8.1.1

Copyright (C) 2018 Free Software Foundation, Inc.

License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software: you are free to change and redistribute it.

There is NO WARRANTY, to the extent permitted by law. Type "show copying"

and "show warranty" for details.

This GDB was configured as "x86\_64-linux-gnu".

Type "show configuration" for configuration details.

For bug reporting instructions, please see:

<http://www.gnu.org/software/gdb/bugs/>.

Find the GDB manual and other documentation resources online at:

<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".

Type "apropos word" to search for commands related to "word"...

Reading symbols from bomb...done.

**// We set the breakpoint here so that the bomb doesn’t explode**

(gdb) b phase\_1

Breakpoint 1 at 0x400e8d

(gdb) b explode\_bomb

Breakpoint 2 at 0x40143d

(gdb) run

Starting program: /mnt/d/one drive/OneDrive/Desktop/12190094/Assignment 1/bomb001/bomb

Welcome to my fiendish little bomb. You have 6 phases with

which to blow yourself up. Have a nice day!

TsheringDuba

Breakpoint 1, 0x0000000000400e8d in phase\_1 ()

(gdb) disas

Dump of assembler code for function phase\_1:

=> 0x0000000000400e8d <+0>: sub $0x8,%rsp

0x0000000000400e91 <+4>: mov $0x4023d0,%esi

**// It compares the input with the answer we provide and from here we know the input is string.**

0x0000000000400e96 <+9>: callq 0x40133e <strings\_not\_equal>

0x0000000000400e9b <+14>: test %eax,%eax

0x0000000000400e9d <+16>: je 0x400ea4 <phase\_1+23>

0x0000000000400e9f <+18>: callq 0x40143d <explode\_bomb>

0x0000000000400ea4 <+23>: add $0x8,%rsp

0x0000000000400ea8 <+27>: retq

End of assembler dump.

**// since we know that it stores a string, we want to get the string stored in the address 0x4023d0 so we use x/s followed by the address.**

(gdb) x/s 0x4023d0

0x4023d0: "The moon unit will be divided into two divisions." **// string stored in the address.**

(gdb) run

The program being debugged has been started already.

Start it from the beginning? (y or n) y

Starting program: /mnt/d/one drive/OneDrive/Desktop/12190094/Assignment 1/bomb001/bomb

Welcome to my fiendish little bomb. You have 6 phases with

which to blow yourself up. Have a nice day!

The moon unit will be divided into two divisions.

Breakpoint 1, 0x0000000000400e8d in phase\_1 ()

(gdb) i b

Num Type Disp Enb Address What

1 breakpoint keep y 0x0000000000400e8d <phase\_1>

breakpoint already hit 1 time

2 breakpoint keep y 0x000000000040143d <explode\_bomb>

(gdb) del 1 **// it is used to delete the breakpoint**

(gdb) run

The program being debugged has been started already.

Start it from the beginning? (y or n) y

Starting program: /mnt/d/one drive/OneDrive/Desktop/12190094/Assignment 1/bomb001/bomb

Welcome to my fiendish little bomb. You have 6 phases with

which to blow yourself up. Have a nice day!

The moon unit will be divided into two divisions.

Phase 1 defused. How about the next one?