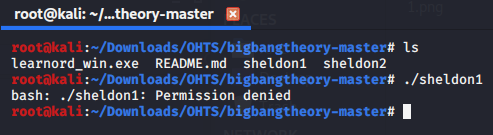
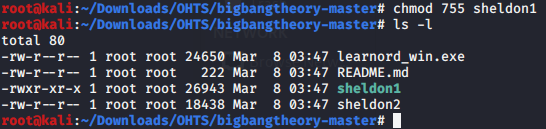
**Sheldon1 Reverse Engineering**

Sheldon1 file contains 6 phases that require various inputs to pass each level. The only way to find each input relevant to each phase reversing the file.

Sheldon1 file cannot run like a standard program because it requires executable permission.

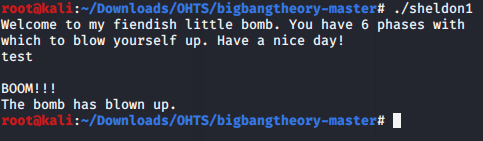


So, the first thing to do is to get the required permission to the file.



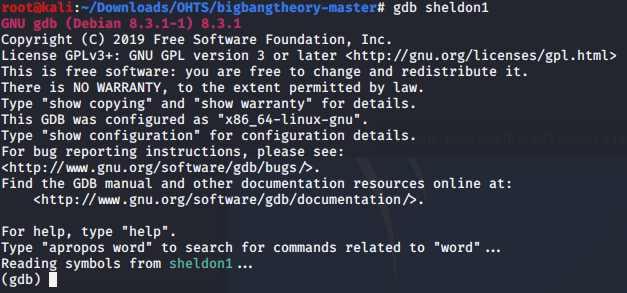
As in the picture above, now Sheldon1 has the executable permission.

After running the sheldon1 file to defuse the bomb, we have to enter some sort of input. If the input is a wrong one, the bomb goes BOOM!!!.

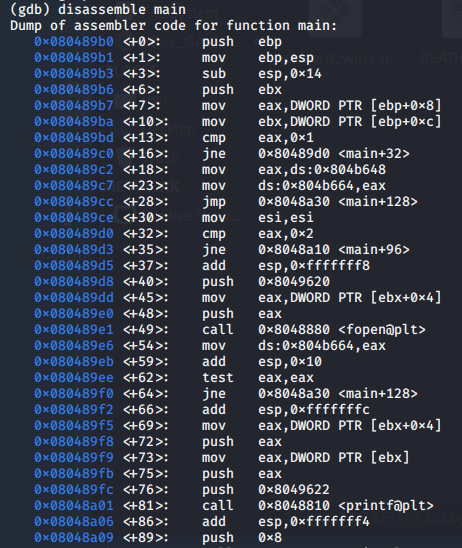


**Phase\_1 Reverse Engineering**

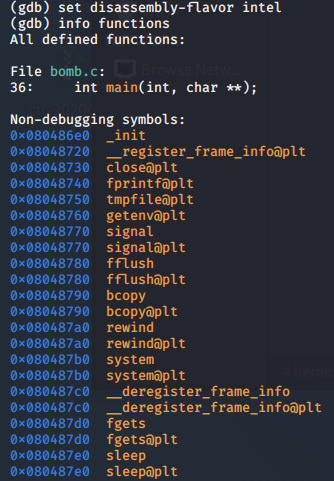
To defuse the bomb, we have to find the correct input. To do that, we can use GDB to reverse engineer the file.

****

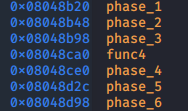
For the first step, we can analyze the main function of the sheldon1 file.



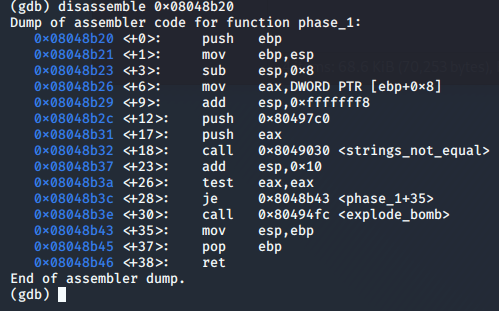
Analyzing the main function is very hard. So the best thing to do is finding the functions



There are many functions in this file. However, if you look closely, you can see the functions for phase 1 to 6.

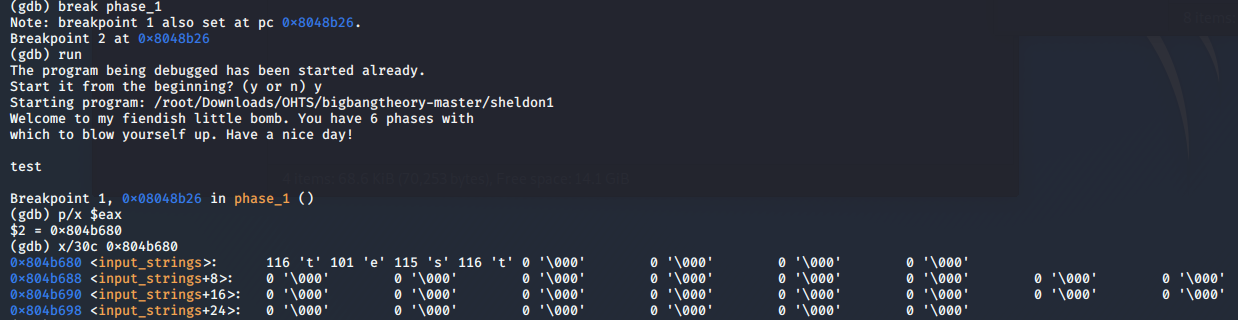


Now we can analyze phase\_1 function to retrieve any information to defuse phase\_1 bomb.



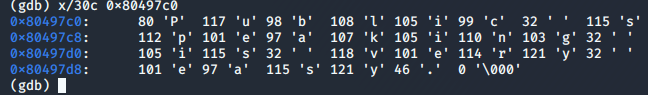
When analyzing the phase\_1 application, we can see there are two values push into the stack before calling the 0x8049030 <string\_not\_equal> function. Those two values are 0x80497c0 location and eax 32bit register. Using GDB, we can retrieve those data.

First, lets set a breakpoint for phase\_1 function and run it. After running the program, we can see the program breaks after calling the phase\_1 function. After that, we can use GDB commands to retrieve the data in those two stack values mentioned above.



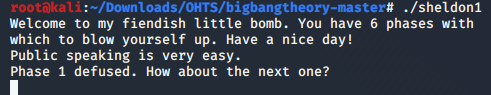
The first location, which is a register, contains information that we entered as the input to the sheldon1 file.

Let's see the second location.



As you can see, the second location contains some sort of string, which appears to be "Public speaking is very easy."

Let's try that string to defuse the bomb.



The first bomb is defused...