PHASE 1 BINARY BOMB

JOHN THOMAS
P2CSN17017

We run the binary bomb in command using gdb ./bomb and run it in peda , it prints out a message.

1. When we analyse the bomb using IDA, we see that from address **08048A3D** which prints **“Welcome to my fiendish little bomb. You have 6 phases with”** and **08048A4A** which prints **“which to blow yourself up. Have a nice day!”-** They both come under the function sub_8049160

2. We see next that 3 functions are called namely **sub_80491FC**, **sub_8048B20** and **sub_804952C**.Then again the printf is called which prints **”Phase 1 defused. How about the next one”...**
   Now we analyse each function in IDA

   sub_80491FC – calls another function **sub_80491B0** which again calls fgets in 080491D3.Thus, we can say that sub_80491FC is used to get the input string.

3. Now when we enter an input , the function **sub_8048B20** check the input string. It checks inside that function and goes to address **0804930** and checks(compares) if the input “**Public speaking is very easy**” is the same as the entered string.Else, it jumbs into the function **sub_80494FC** and calls the printf to displays the output **BOOM!!!** in 0804950A and **The bomb has blown up** in 08049517.

4. Going into the function sub_8048B20,the EAX is storing the entered input.
   A new string is also pushed in the stack so it goes to **sub_0804930** .This contains both the strings ie,the entered and stored string.When we enter into **sub_0804930** ,it has another subfunction in it which calls **sub_8049018** .

5. We see that there are 2 arguments passed before the function **sub_8049018** is executed**.**
   Both values in arguments are different with mov esi, [ebp+arg_0] and mov, esi,[ebp+arg_4].
   Now when we go into **sub_8049018** ,it calculates the length of the string stored in stack .
   It then compares the string length.If the compare gives 0, then strings are equal.So it goes to the function **loc_8048B43** which ends it and calls the printf in **sub_804952C** which prints **Phase 1 defused , How about next one.**Else if compare gives 1 it goes back to **sub_80494FC** again and displays the bomb has blown up.