Question Set 0x07

HQS Challenge

January 22, 2016

This is a practical exercise. This entire exercise should be observed by the person signing off the HQS item.
To answer the following questions download this binary: chal0x01 or `https://goo.gl/ItW84O`

1. Run the program with gdb
2. Add a breakpoint for the main function
3. Begin program execution (it will break at the breakpoint added above)
4. Change the disassembly flavor to Intel syntax.
5. Disassemble the current function and find the address of the instruction immediately following the call to __isoc99_scanf
6. Set a breakpoint for that instruction (use the address you just found)
7. Continue program execution until it breaks on the new breakpoint, for the password enter 'test_password'
8. Examine the string located at this address: `$rbp-0x40`
9. What string is this?
10. Now examine the string at this address: `0x4007da`
11. What is this? Is is significant?
12. Exit gdb and re-run the program with the string from above as input. What happens?

Solutions

1. `$ gdb -q chal0x01`
2. `(gdb) break main`
3. `(gdb) r`

4. `(gdb) set disassembly-flavor intel`
5. `(gdb) disass`
6. `(gdb) break *0x00000000004006e1`
7. `(gdb) x/s $rbp-0x40`
8. This is the password we just entered
9. `(gdb) x/s 0x4007da`
10. This is the real password the program is looking for - verified by the later call to `strncmp()`
11. `(gdb) quit` - It accepts the password, congragulations!