Question Set 0x09

HQS Challenge

January 22, 2016

This is a practical exercise. It should be observed in its entirety by the person signing off the HQS item.
For the following questions download this binary: chal0x02 or `https://goo.gl/z1Oohl`

1. Run the program in radare2 - make sure it is attached to a process
2. Add a breakpoint for the 'main' function
3. Execute the program until the breakpoint is reached
4. Disassemble the program and find the address of the instruction `xor eax, eax`
5. Set a breakpoint for that address
6. Continue execution until that breakpoint is reached
7. Single step to the next instruction
8. Examine the current values at `rbp-0x50` - they should all be 0x00
9. Single step to the next instruction
10. Repeat the above two steps about 5 times - what is happening?
11. What is the password after it is fully loaded?

Solutions

1. `$ r2 -d ./chal0x02`
2. `[0x...]> db main`
3. `[0x...]> dc`
4. `[0x0040069d]> pd @ main`
5. `[0x0040069d]> db 0x04006ba`

6. `[0x0040069d]> dc`
7. `[0x0040069d]> ds`
8. `[0x0040069d]> px @ rbp-0x50`
9. `[0x0040069d]> ds`
10. ... The password is being loaded in one byte at a time.
11. `that_isn't_any_better`