# Explanation part

=> 0x0804842b <+71>: movl $0x5a,-0x8(%ebp) : 90 -> -0x8 epb

0x08048432 <+78>: movl $0x1ec,-0xc(%ebp) : 492 -> -0xc epb

0x08048439 <+85>: mov -0xc(%ebp),%edx : 492 -> edx

0x0804843c <+88>: lea -0x8(%ebp),%eax : 90 -> eax

0x0804843f <+91>: add %edx,(%eax) : 492+90 -> eax

0x08048441 <+93>: mov -0x8(%ebp),%eax : 0x8(%ebp) = eax = 582

0x08048444 <+96>: imul -0x8(%ebp),%eax : 582 \* 582 = 338724 -> eax

0x08048448 <+100>: mov %eax,-0xc(%ebp) : 338724 -> -0xc epp

0x0804844b <+103>: mov -0x4(%ebp),%eax : scanf number

0x0804844e <+106>: cmp -0xc(%ebp),%eax : compare “338724” with password

# DEBUG Part

vagrant@ubuntu-focal:/vagrant/lab1/IOLI-crackme$ gdb crackme0x02

GNU gdb (Ubuntu 9.2-0ubuntu1~20.04.1) 9.2

Copyright (C) 2020 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 crackme0x02...

(No debugging symbols found in crackme0x02)

(gdb) r

Starting program: /vagrant/lab1/IOLI-crackme/crackme0x02

IOLI Crackme Level 0x02

Password: ^C

Program received signal SIGINT, Interrupt.

0xf7fd0b49 in \_\_kernel\_vsyscall ()

(gdb) bt

#0 0xf7fd0b49 in \_\_kernel\_vsyscall ()

#1 0xf7ec4bab in read () from /lib/i386-linux-gnu/libc.so.6

#2 0xf7e4cc73 in \_IO\_file\_underflow () from /lib/i386-linux-gnu/libc.so.6

#3 0xf7e4e020 in \_IO\_default\_uflow () from /lib/i386-linux-gnu/libc.so.6

#4 0xf7e25829 in ?? () from /lib/i386-linux-gnu/libc.so.6

#5 0xf7e23429 in scanf () from /lib/i386-linux-gnu/libc.so.6

#6 0x0804842b in main ()

(gdb) tbreak \*0x0804842b

Temporary breakpoint 1 at 0x804842b

(gdb) c

Continuing.

12111

Temporary breakpoint 1, 0x0804842b in main ()

(gdb) disas

Dump of assembler code for function main:

0x080483e4 <+0>: push %ebp

0x080483e5 <+1>: mov %esp,%ebp

0x080483e7 <+3>: sub $0x18,%esp

0x080483ea <+6>: and $0xfffffff0,%esp

0x080483ed <+9>: mov $0x0,%eax

0x080483f2 <+14>: add $0xf,%eax

0x080483f5 <+17>: add $0xf,%eax

0x080483f8 <+20>: shr $0x4,%eax

0x080483fb <+23>: shl $0x4,%eax

0x080483fe <+26>: sub %eax,%esp

0x08048400 <+28>: movl $0x8048548,(%esp)

0x08048407 <+35>: call 0x804831c <printf@plt>

0x0804840c <+40>: movl $0x8048561,(%esp)

0x08048413 <+47>: call 0x804831c <printf@plt>

0x08048418 <+52>: lea -0x4(%ebp),%eax

0x0804841b <+55>: mov %eax,0x4(%esp)

0x0804841f <+59>: movl $0x804856c,(%esp)

0x08048426 <+66>: call 0x804830c <scanf@plt>

=> 0x0804842b <+71>: movl $0x5a,-0x8(%ebp)

0x08048432 <+78>: movl $0x1ec,-0xc(%ebp)

0x08048439 <+85>: mov -0xc(%ebp),%edx

0x0804843c <+88>: lea -0x8(%ebp),%eax

0x0804843f <+91>: add %edx,(%eax)

0x08048441 <+93>: mov -0x8(%ebp),%eax

0x08048444 <+96>: imul -0x8(%ebp),%eax

0x08048448 <+100>: mov %eax,-0xc(%ebp)

0x0804844b <+103>: mov -0x4(%ebp),%eax

0x0804844e <+106>: cmp -0xc(%ebp),%eax

--Type <RET> for more, q to quit, c to continue without paging--

0x08048451 <+109>: jne 0x8048461 <main+125>

0x08048453 <+111>: movl $0x804856f,(%esp)

0x0804845a <+118>: call 0x804831c <printf@plt>

0x0804845f <+123>: jmp 0x804846d <main+137>

0x08048461 <+125>: movl $0x804857f,(%esp)

0x08048468 <+132>: call 0x804831c <printf@plt>

0x0804846d <+137>: mov $0x0,%eax

0x08048472 <+142>: leave

0x08048473 <+143>: ret

End of assembler dump.

(gdb) p 0x5a

$1 = 90

(gdb) p 0x1ec

$2 = 492

# Check password

(gdb) r

(gdb) ogram being debugged has been started already.

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

(gdb) ng program: /vagrant/lab1/IOLI-crackme/crackme0x02

(gdb) rackme Level 0x02

(gdb) rd: 338724

(gdb) rd OK :)