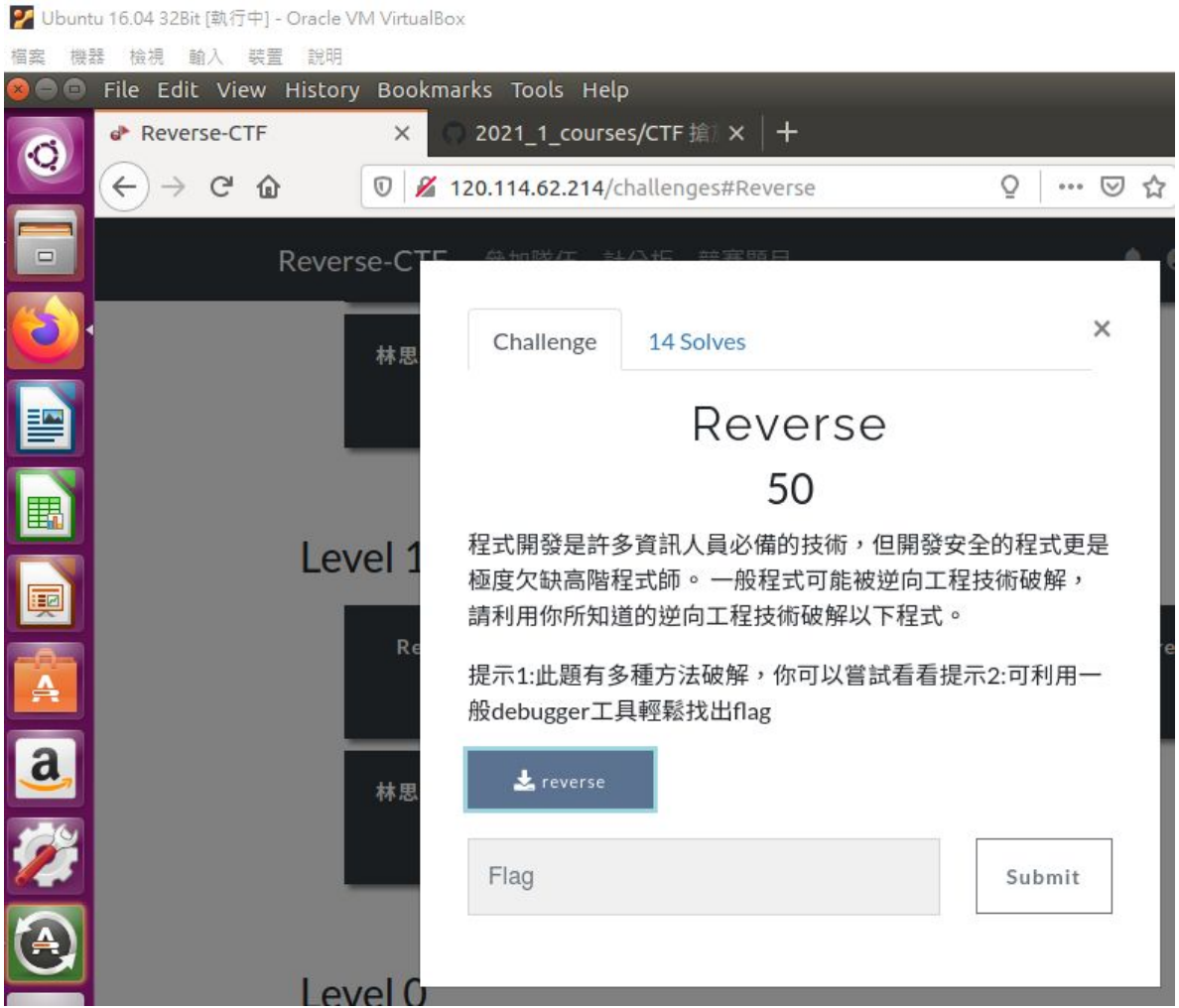
CTF
2021 03 13

http://120.114.62.214/challenges

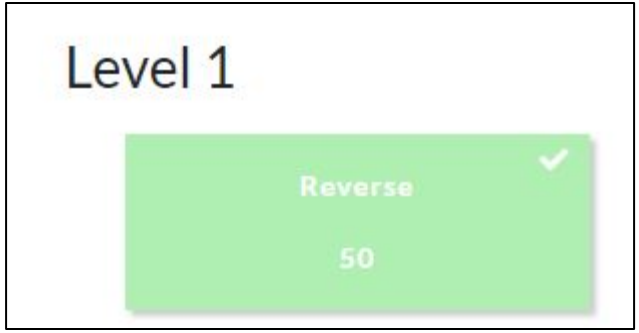

Ubuntu 16.04 32Bit [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
File Edit View History Bookmarks Tools Help
Reverse-CTF
2021_1_courses/CTF
120.114.62.214/challenges#Reverse
Challenge
14 Solves
Reverse
50
程式開發是許多資訊人員必備的技術，但開發安全的程式更是極度欠缺高階程式師。一般程式可能被逆向工程技術破解，請利用你所知道的逆向工程技術破解以下程式。
提示1:此題有多種方法破解，你可以嘗試看看提示2:可利用一般debugger工具輕鬆找出flag
reverse
Flag
Submit

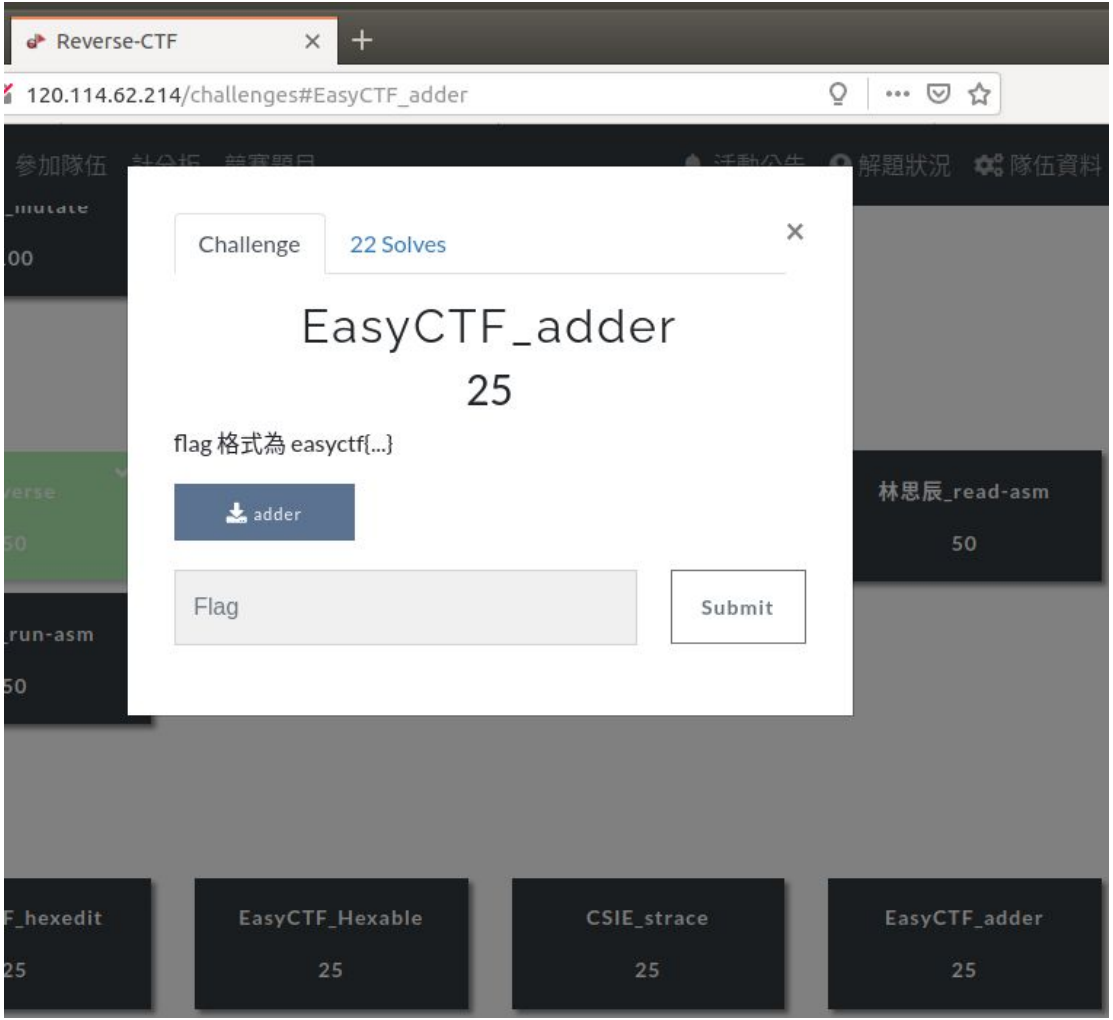
Ubuntu 16.04 32Bit [執行中] - Oracle VM VirtualBox

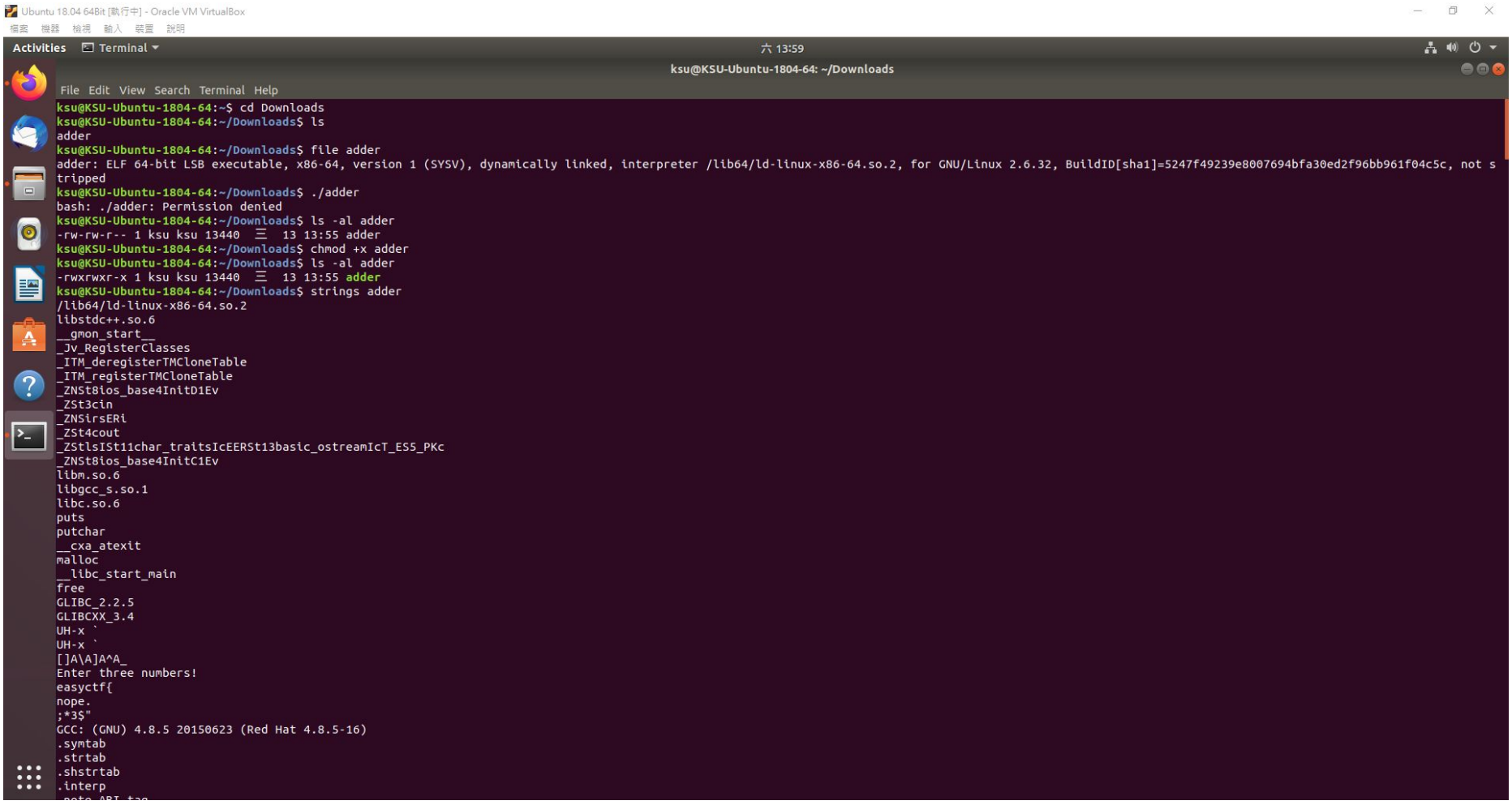
檔案 機器 檢視 輸入 裝置 說明

```
ksu@KSU-Ubuntu-1604-32:~$ cd Downloads
ksu@KSU-Ubuntu-1604-32:~/Downloads$ ls
adder         ezreverse  hexedit  LuckyGuess  strace
Coffee.class  hexable    liar     reverse
ksu@KSU-Ubuntu-1604-32:~/Downloads$ file reverse
reverse: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linu
x.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=0eae3e9fd6d9a63980d737561cba79a68e655c9f, not stripped
ksu@KSU-Ubuntu-1604-32:~/Downloads$ ls -al reverse
-rw-rw-r-- 1 ksu ksu 7380  三  13 11:32 reverse
ksu@KSU-Ubuntu-1604-32:~/Downloads$ chmod +x reverse
ksu@KSU-Ubuntu-1604-32:~/Downloads$ ls -al reverse
-rwxrwxr-x 1 ksu ksu 7380  三  13 11:32 reverse
ksu@KSU-Ubuntu-1604-32:~/Downloads$ strings reverse
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
gets
puts
__libc_start_main
__gmon_start__
GLIBC_2.0
PTRh
QVh;
UWVS
t$,U
[^_]
BreakALLCTF{4U49uY7OJCrJL0vtbXjd}
Try again?
;*2$"(
GCC: (Ubuntu 5.4.0-6ubuntu1~16.04.4) 5.4.0 20160609
crtstuff.c
__JCR_LIST__
deregister_tm_clones
__do_global_dtors_aux
completed.7200
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
re-1.c
__FRAME_END__
__JCR_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
__x86.get_pc_thunk.bx
gets@@GLIBC_2.0
_edata
__data_start
puts@@GLIBC_2.0
__gmon_start__
__dso_handle
_IO_stdin_used
```

```
__libc_start_main@@GLIBC_2.0
__libc_csu_init
_fp_hw
__bss_start
main
_Jv_RegisterClasses
__TMC_END__
_ITM_registerTMCloneTable
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rel.dyn
.rel.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.jcr
.dynamic
.got.plt
.data
.bss
.comment
ksu@KSU-Ubuntu-1604-32:~/Downloads$
```



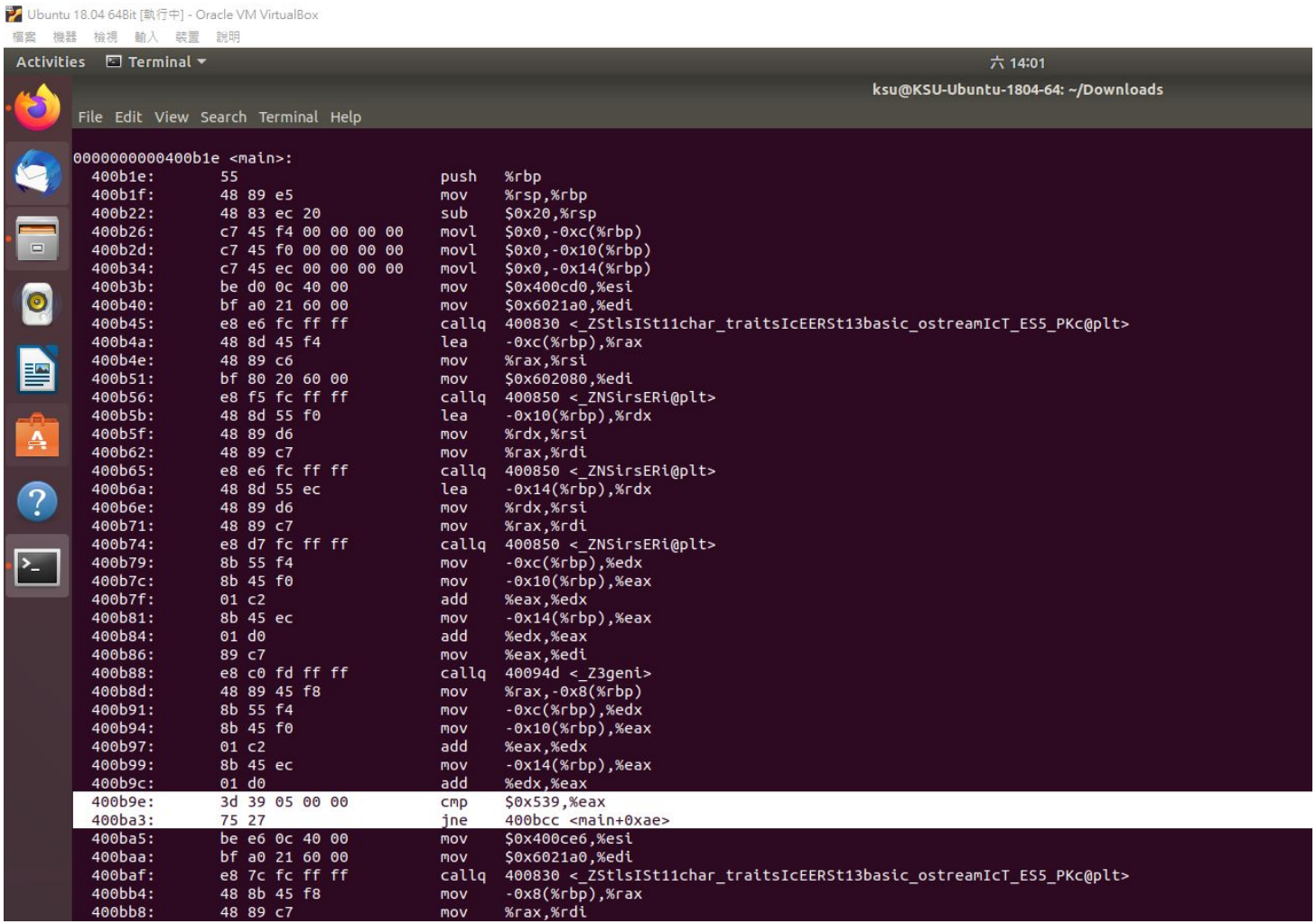

Reverse-CTF
120.114.62.214/challenges#EasyCTF_adder
參加隊伍
解題狀況
隊伍資料
Challenge
22 Solves
EasyCTF_adder
25
flag 格式為 easyctf{...}
adder
Flag
Submit
林思辰_read-asm
50
EasyCTF_Hexable
25
CSIE_strace
25
EasyCTF_adder
25


Ubuntu 18.04 64Bit [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
Activities
Terminal
六 13:59
ksu@KSU-Ubuntu-1804-64: ~/Downloads
File Edit View Search Terminal Help
ksu@KSU-Ubuntu-1804-64:~$ cd Downloads
ksu@KSU-Ubuntu-1804-64:~/Downloads$ ls
adder
ksu@KSU-Ubuntu-1804-64:~/Downloads$ file adder
adder: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=5247f49239e8007694bfa30ed2f96bb961f04c5c, not s
tripped
ksu@KSU-Ubuntu-1804-64:~/Downloads$ ./adder
bash: ./adder: Permission denied
ksu@KSU-Ubuntu-1804-64:~/Downloads$ ls -al adder
-rw-rw-r-- 1 ksu ksu 13440 三 13 13:55 adder
ksu@KSU-Ubuntu-1804-64:~/Downloads$ chmod +x adder
ksu@KSU-Ubuntu-1804-64:~/Downloads$ ls -al adder
-rwxrwxr-x 1 ksu ksu 13440 三 13 13:55 adder
ksu@KSU-Ubuntu-1804-64:~/Downloads$ strings adder
/lib64/ld-linux-x86-64.so.2
libstdc++.so.6
__gmon_start__
_Jv_RegisterClasses
_ITM_deregisterTMCloneTable
_ITM_registerTMCloneTable
_ZNSt8ios_base4InitD1Ev
_ZSt3cin
_ZNSirsERi
_ZSt4cout
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc
_ZNSt8ios_base4InitC1Ev
libm.so.6
libgcc_s.so.1
libc.so.6
puts
putchar
__cxa_atexit
malloc
__libc_start_main
free
GLIBC_2.2.5
GLIBCXX_3.4
UH-x `
UH-x `
[]A\A]A^A_
Enter three numbers!
easyctf{
nope.
;*3$"
GCC: (GNU) 4.8.5 20150623 (Red Hat 4.8.5-16)
.symtab
.strtab
.shstrtab
.interp

ksu@KSU-Ubuntu-1804-64: ~/Downloads

File Edit View Search Terminal Help

```
ksu@KSU-Ubuntu-1804-64:~/Downloads$ objdump -S adder

adder:     file format elf64-x86-64


Disassembly of section .init:

0000000000400778 <_init>:
  400778:       48 83 ec 08             sub    $0x8,%rsp
  40077c:       48 8b 05 75 18 20 00    mov    0x201875(%rip),%rax        # 601ff8 <__gmon_start__>
  400783:       48 85 c0                test   %rax,%rax
  400786:       74 05                   je     40078d <_init+0x15>
  400788:       e8 23 00 00 00          callq  4007b0 <__gmon_start__@plt>
  40078d:       48 83 c4 08             add    $0x8,%rsp
  400791:       c3                      retq

Disassembly of section .plt:

00000000004007a0 <.plt>:
  4007a0:       ff 35 62 18 20 00       pushq  0x201862(%rip)        # 602008 <_GLOBAL_OFFSET_TABLE_+0x8>
  4007a6:       ff 25 64 18 20 00       jmpq   *0x201864(%rip)        # 602010 <_GLOBAL_OFFSET_TABLE_+0x10>
  4007ac:       0f 1f 40 00             nopl   0x0(%rax)

00000000004007b0 <__gmon_start__@plt>:
  4007b0:       ff 25 62 18 20 00       jmpq   *0x201862(%rip)        # 602018 <__gmon_start__>
  4007b6:       68 00 00 00 00          pushq  $0x0
  4007bb:       e9 e0 ff ff ff          jmpq   4007a0 <.plt>

00000000004007c0 <puts@plt>:
  4007c0:       ff 25 5a 18 20 00       jmpq   *0x20185a(%rip)        # 602020 <puts@GLIBC_2.2.5>
  4007c6:       68 01 00 00 00          pushq  $0x1
  4007cb:       e9 d0 ff ff ff          jmpq   4007a0 <.plt>

00000000004007d0 <putchar@plt>:
  4007d0:       ff 25 52 18 20 00       jmpq   *0x201852(%rip)        # 602028 <putchar@GLIBC_2.2.5>
  4007d6:       68 02 00 00 00          pushq  $0x2
  4007db:       e9 c0 ff ff ff          jmpq   4007a0 <.plt>

00000000004007e0 <_ZNSt8ios_base4InitC1Ev@plt>:
  4007e0:       ff 25 4a 18 20 00       jmpq   *0x20184a(%rip)        # 602030 <_ZNSt8ios_base4InitC1Ev@GLIBCXX_3.4>
  4007e6:       68 03 00 00 00          pushq  $0x3
  4007eb:       e9 b0 ff ff ff          jmpq   4007a0 <.plt>

00000000004007f0 <malloc@plt>:
  4007f0:       ff 25 42 18 20 00       jmpq   *0x201842(%rip)        # 602038 <malloc@GLIBC_2.2.5>
  4007f6:       68 04 00 00 00          pushq  $0x4
  4007fb:       e9 a0 ff ff ff          jmpq   4007a0 <.plt>

0000000000400800 <__libc_start_main@plt>:
  400800:       ff 25 3a 18 20 00       jmpq   *0x20183a(%rip)        # 602040 <__libc_start_main@GLIBC_2.2.5>
```


Ubuntu 18.04 64Bit [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
Activities
Terminal
六 14:01
ksu@KSU-Ubuntu-1804-64: ~/Downloads
File Edit View Search Terminal Help
0000000000400b1e <main>:
400b1e: 55 push %rbp
400b1f: 48 89 e5 mov %rsp,%rbp
400b22: 48 83 ec 20 sub $0x20,%rsp
400b26: c7 45 f4 00 00 00 00 movl $0x0,-0xc(%rbp)
400b2d: c7 45 f0 00 00 00 00 movl $0x0,-0x10(%rbp)
400b34: c7 45 ec 00 00 00 00 movl $0x0,-0x14(%rbp)
400b3b: be d0 0c 40 00 mov $0x400cd0,%esi
400b40: bf a0 21 60 00 mov $0x6021a0,%edi
400b45: e8 e6 fc ff ff callq 400830 <_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc@plt>
400b4a: 48 8d 45 f4 lea -0xc(%rbp),%rax
400b4e: 48 89 c6 mov %rax,%rsi
400b51: bf 80 20 60 00 mov $0x602080,%edi
400b56: e8 f5 fc ff ff callq 400850 <_ZNSirsERi@plt>
400b5b: 48 8d 55 f0 lea -0x10(%rbp),%rdx
400b5f: 48 89 d6 mov %rdx,%rsi
400b62: 48 89 c7 mov %rax,%rdi
400b65: e8 e6 fc ff ff callq 400850 <_ZNSirsERi@plt>
400b6a: 48 8d 55 ec lea -0x14(%rbp),%rdx
400b6e: 48 89 d6 mov %rdx,%rsi
400b71: 48 89 c7 mov %rax,%rdi
400b74: e8 d7 fc ff ff callq 400850 <_ZNSirsERi@plt>
400b79: 8b 55 f4 mov -0xc(%rbp),%edx
400b7c: 8b 45 f0 mov -0x10(%rbp),%eax
400b7f: 01 c2 add %eax,%edx
400b81: 8b 45 ec mov -0x14(%rbp),%eax
400b84: 01 d0 add %edx,%eax
400b86: 89 c7 mov %eax,%edi
400b88: e8 c0 fd ff ff callq 40094d <_Z3geni>
400b8d: 48 89 45 f8 mov %rax,-0x8(%rbp)
400b91: 8b 55 f4 mov -0xc(%rbp),%edx
400b94: 8b 45 f0 mov -0x10(%rbp),%eax
400b97: 01 c2 add %eax,%edx
400b99: 8b 45 ec mov -0x14(%rbp),%eax
400b9c: 01 d0 add %edx,%eax
400b9e: 3d 39 05 00 00 cmp $0x539,%eax
400ba3: 75 27 jne 400bcc <main+0xae>
400ba5: be e6 0c 40 00 mov $0x400ce6,%esi
400baa: bf a0 21 60 00 mov $0x6021a0,%edi
400baf: e8 7c fc ff ff callq 400830 <_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc@plt>
400bb4: 48 8b 45 f8 mov -0x8(%rbp),%rax
400bb8: 48 89 c7 mov %rax,%rdi

I have the following src:

```
1  #include<stdio.h>
2
3  int main(void) {
4      int i= 1337; // breakpoint after this value is assigned
!5     return 0;
6  }
```

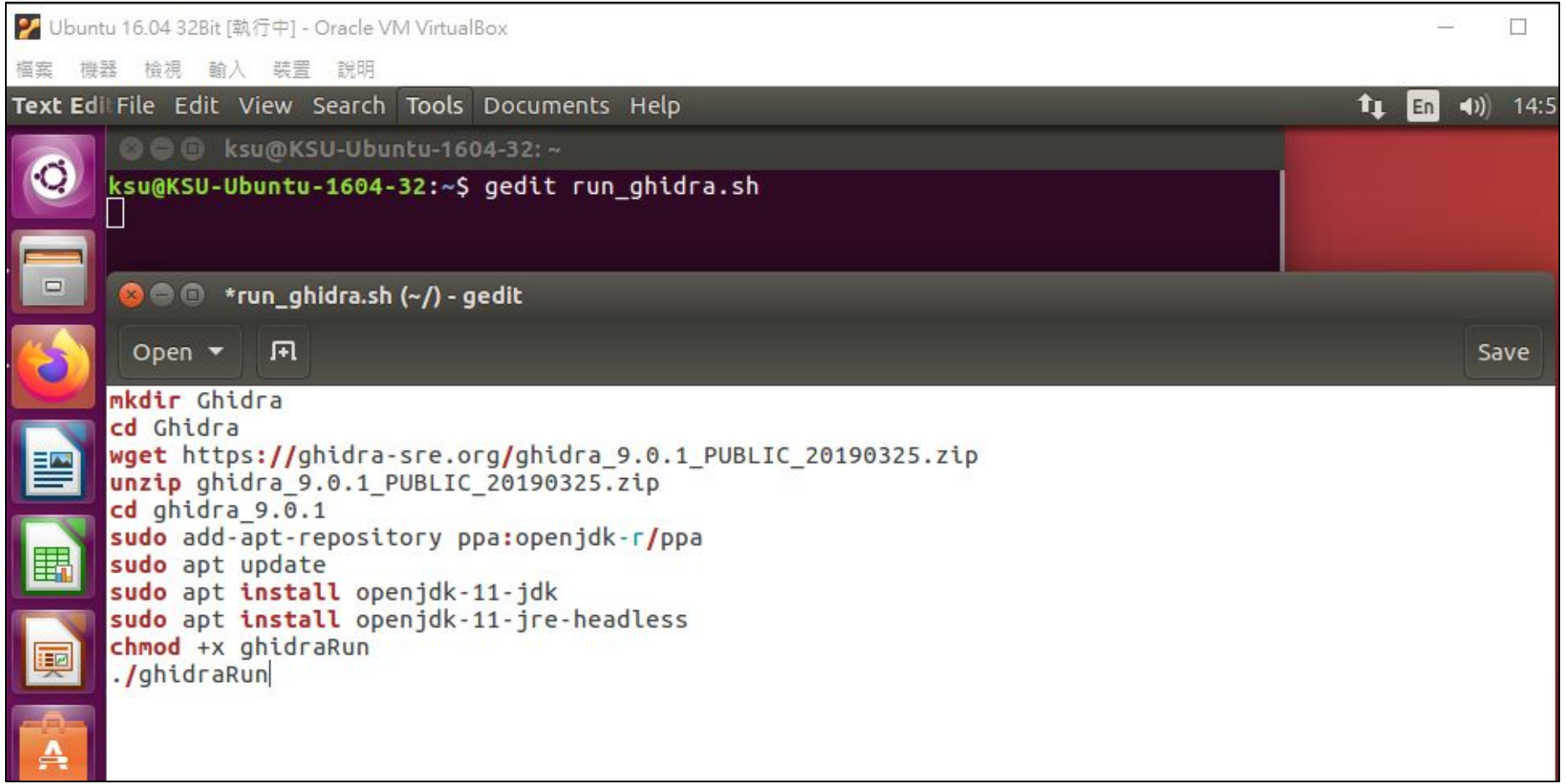
In the asm from `gdb` I get:

```
ksu@KSU-Ubuntu-1804-64:~/Downloads$ ./adder
Enter three numbers!
1337
0
0
easyctf{y0u_added_thr33_nums!}
ksu@KSU-Ubuntu-1804-64:~/Downloads$
```

```
!0x0000000004004f1  main+4  movl   $0x539,-0x4(%rbp)
```

And I verified that `$0x539` = `1337`. How can I see the memory address where the value `1337` is stored? The value of the `rbp` memory address shows:

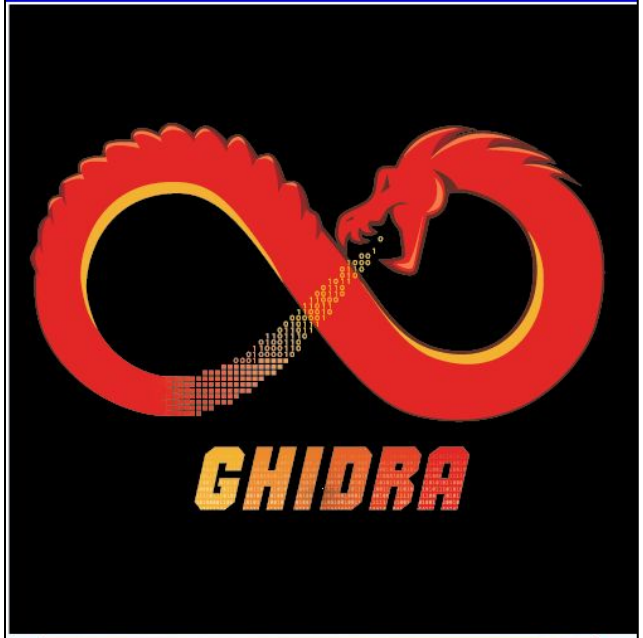
```
rbp 0x00007fffffffeb20
```


Ubuntu 16.04 32Bit [執行中] - Oracle VM VirtualBox
檔案 機器 檢視 輸入 裝置 說明
Text Edi File Edit View Search Tools Documents Help
En
14:5
ksu@KSU-Ubuntu-1604-32: ~
ksu@KSU-Ubuntu-1604-32:~$ gedit run_ghidra.sh
*run_ghidra.sh (~/) - gedit
Open
Save
mkdir Ghidra
cd Ghidra
wget https://ghidra-sre.org/ghidra_9.0.1_PUBLIC_20190325.zip
unzip ghidra_9.0.1_PUBLIC_20190325.zip
cd ghidra_9.0.1
sudo add-apt-repository ppa:openjdk-r/ppa
sudo apt update
sudo apt install openjdk-11-jdk
sudo apt install openjdk-11-jre-headless
chmod +x ghidraRun
./ghidraRun

```
ksu@KSU-Ubuntu-1604-32:~$ chmod +x run_ghidra.sh
ksu@KSU-Ubuntu-1604-32:~$ ./run_ghidra.sh
--2021-03-13 14:56:09--  https://ghidra-sre.org/ghidra_9.0.1_PUBLIC_20190325.zip
Resolving ghidra-sre.org (ghidra-sre.org)... 13.227.73.28, 13.227.73.84, 13.227.73.9, ...
Connecting to ghidra-sre.org (ghidra-sre.org)|13.227.73.28|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 296076039 (282M) [application/zip]
Saving to: ‘ghidra_9.0.1_PUBLIC_20190325.zip’

ghidra_9.0.1_PUBLIC 100%[===================>] 282.36M  2.73MB/s    in 64s

2021-03-13 14:57:14 (4.40 MB/s) - ‘ghidra_9.0.1_PUBLIC_20190325.zip’ saved [296076039/296076039]

Archive:  ghidra_9.0.1_PUBLIC_20190325.zip
   creating: ghidra_9.0.1/
  inflating: ghidra_9.0.1/ghidraRun.bat
  inflating: ghidra_9.0.1/ghidraRun
   creating: ghidra_9.0.1/licenses/
  inflating: ghidra_9.0.1/licenses/Modified_Nuvola_Icons_-_LGPL_2.1.txt
  inflating: ghidra_9.0.1/licenses/Tango_Icons_-_Public_Domain.txt
  inflating: ghidra_9.0.1/licenses/Nuvola_Icons_-_LGPL_2.1.txt
  inflating: ghidra_9.0.1/licenses/Oxygen_Icons_-_LGPL_3.0.txt
  inflating: ghidra_9.0.1/licenses/LGPL_2.1.txt
  inflating: ghidra_9.0.1/licenses/GPL_2_With_Classpath_Exception.txt
  inflating: ghidra_9.0.1/licenses/Public_Domain.txt
  inflating: ghidra_9.0.1/licenses/Jython_License.txt
  inflating: ghidra_9.0.1/licenses/JDOM_License.txt
  inflating: ghidra_9.0.1/licenses/Apache_License_2.0.txt
  inflating: ghidra_9.0.1/licenses/FAMFAMFAM_MINI_ICONS_-_Public_Domain.txt
  inflating: ghidra_9.0.1/licenses/MIT.txt
  inflating: ghidra_9.0.1/licenses/BSD.txt
  inflating: ghidra_9.0.1/licenses/Christian_Plattner.txt
  inflating: ghidra_9.0.1/licenses/Crystal_Clear_Icons_-_LGPL_2.1.txt
  inflating: ghidra_9.0.1/licenses/Creative_Commons_Attribution_2.5.html
  inflating: ghidra_9.0.1/licenses/FAMFAMFAM_Icons_-_CC_2.5.txt
  inflating: ghidra_9.0.1/licenses/LGPL_3.0.html
```

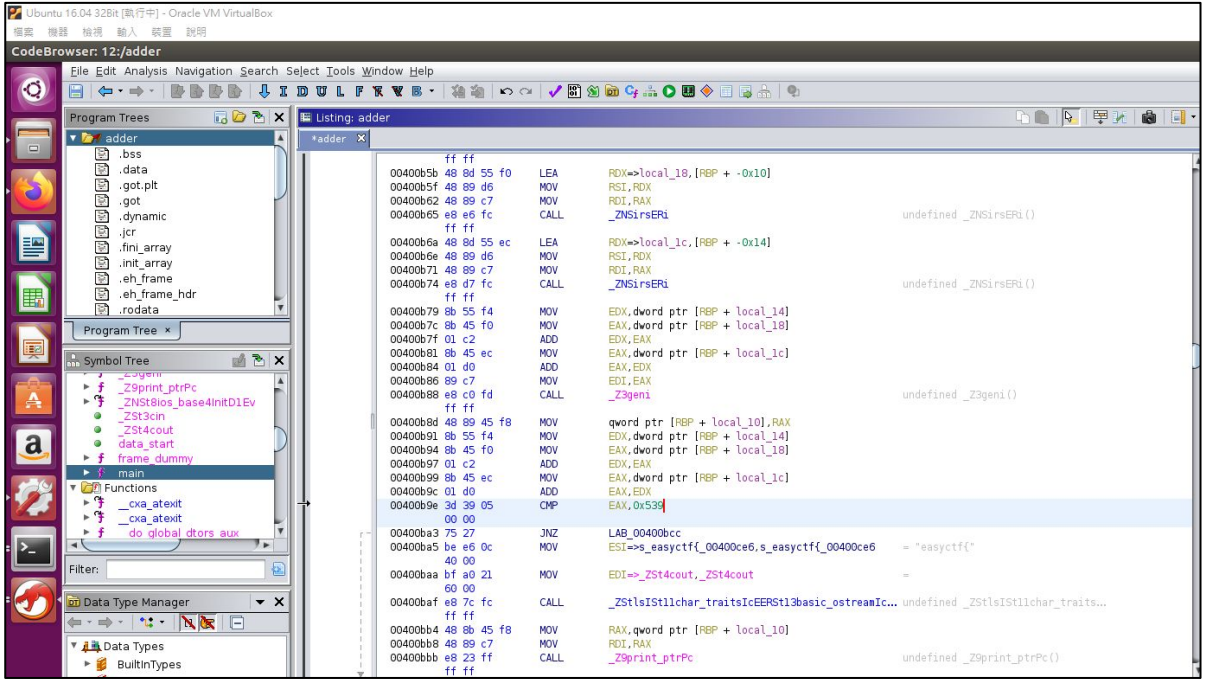

Ghidra User Agreement
Licensed under the Apache License, Version 2.0 (the "License"); Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.
As a software reverse engineering (SRE) framework, Ghidra is designed solely to facilitate lawful SRE activities. You should always ensure that any SRE activities in which you engage are permissible as computer software may be protected under governing law (e.g., copyright) or under an applicable licensing agreement. In making Ghidra available for public use, the National Security Agency does not condone or encourage any improper usage of Ghidra. Consistent with the Apache 2.0 license under which Ghidra has been made available, you are solely responsible for determining the appropriateness of using or redistributing Ghidra.
I Agree
I Don't Agree
Reading state information... Done
openjdk-11-jre-headless is already the newest version (11.0.11+4-0ubuntu3~16.04~1).
openjdk-11-jre-headless set to manually installed.
The following package was automatically installed and is no longer required:
snapd-login-service
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
ksu@KSU-Ubuntu-1604-32:~$

Welcome To Ghidra



Version 9.0.1
Build PUBLIC
2019-Mar-25 1752 EDT
Java Version 11.0.11-ea

Scanning jar: DATA.jar


Ubuntu 16.04 32Bit [執行中] - Oracle VM VirtualBox
CodeBrowser: 12:/adder
File Edit Analysis Navigation Search Select Tools Window Help
Program Trees
adder
.bss
.data
.got.plt
.got
.dynamic
.jcr
.fini_array
.init_array
.eh_frame
.eh_frame_hdr
.rodata
Program Tree
Symbol Tree
_Z9print_ptrPc
_ZNSt8ios_base4InitD1Ev
_ZSt3cin
_ZSt4cout
data_start
frame_dummy
main
Functions
__cxa_atexit
__cxa_atexit
__do_global_dtors_aux
Filter:
Data Type Manager
Data Types
BuiltInTypes
Listing: adder
*adder
ff ff
00400b5b 48 8d 55 f0 LEA RDX=>local_18,[RBP + -0x10]
00400b5f 48 89 d6 MOV RSI,RDX
00400b62 48 89 c7 MOV RDI,RAX
00400b65 e8 e6 fc CALL _ZNSirsERi undefined _ZNSirsERi()
ff ff
00400b6a 48 8d 55 ec LEA RDX=>local_1c,[RBP + -0x14]
00400b6e 48 89 d6 MOV RSI,RDX
00400b71 48 89 c7 MOV RDI,RAX
00400b74 e8 d7 fc CALL _ZNSirsERi undefined _ZNSirsERi()
ff ff
00400b79 8b 55 f4 MOV EDX,dword ptr [RBP + local_14]
00400b7c 8b 45 f0 MOV EAX,dword ptr [RBP + local_18]
00400b7f 01 c2 ADD EDX,EAX
00400b81 8b 45 ec MOV EAX,dword ptr [RBP + local_1c]
00400b84 01 d0 ADD EAX,EDX
00400b86 89 c7 MOV EDI,EAX
00400b88 e8 c0 fd CALL _Z3geni undefined _Z3geni()
ff ff
00400b8d 48 89 45 f8 MOV qword ptr [RBP + local_10],RAX
00400b91 8b 55 f4 MOV EDX,dword ptr [RBP + local_14]
00400b94 8b 45 f0 MOV EAX,dword ptr [RBP + local_18]
00400b97 01 c2 ADD EDX,EAX
00400b99 8b 45 ec MOV EAX,dword ptr [RBP + local_1c]
00400b9c 01 d0 ADD EAX,EDX
00400b9e 3d 39 05 CMP EAX,0x539
00 00
00400ba3 75 27 JNZ LAB_00400bcc
00400ba5 be e6 0c MOV ESI=>s_easyctf{_00400ce6,s_easyctf{_00400ce6 = "easyctf{"
40 00
00400baa bf a0 21 MOV EDI=>_ZSt4cout,_ZSt4cout =
60 00
00400baf e8 7c fc CALL _ZStlsISt11char_traitsIcEERSt13basic_ostreamIc... undefined _ZStlsISt11char_traits...
ff ff
00400bb4 48 8b 45 f8 MOV RAX,qword ptr [RBP + local_10]
00400bb8 48 89 c7 MOV RDI,RAX
00400bbb e8 23 ff CALL _Z9print_ptrPc undefined _Z9print_ptrPc()
ff ff