

# ebCTF bin200 Writeup

原创

[0x4C43](#) 于 2016-08-10 19:48:24 发布 625 收藏 2

分类专栏: [逆向工程 CTF](#) 文章标签: [二进制 CTF bin](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/swjtu100/article/details/52175583>

版权



[逆向工程](#) 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏



[CTF](#)

2 篇文章 0 订阅

订阅专栏

刚接触CTF, 做了一道简单的逆向题 ([题目链接](#))。这道题是一个掷骰子的游戏, 只要能掷出一串特定的值就能得到flag。

```
[*] ebCTF 2013 Teaser - BIN100 - Dice Game
    To get the flag you will need to throw the correct numbers.

[*] You will first need to throw a three, press enter to throw a dice!

-----
| 0  0 |
| 0  0 |
| 0  0 |
-----

[*] You rolled a 6 That is not a three :/
[*] Game over!
```

## 0x01 IDA加载分析

使用IDA加载二进制文件, 打开Strings window查看字符串。

| Address         | Length   | Type | String  |
|-----------------|----------|------|---|
| .rdata:0044416C | 0000002B | C    | [*] ebCTF 2013 Teaser - BIN100 - Dice Game  |
| .rdata:00444198 | 00000040 | C    | To get the flag you will need to throw the correct numbers.                               |
| .rdata:004441D8 | 00000047 | C    | [*] You will first need to throw a three, press enter to throw a dice!                    |
| .rdata:0044421F | 0000001E | C    | [*] You rolled a three! Good!   |
| .rdata:00444244 | 00000009 | C    | =3WG-'jsD   |
| .rdata:0044425B | 00000006 | C    | JxtjpB  |
| .rdata:00444268 | 00000012 | C    | [*] You rolled a  |
| .rdata:0044427A | 00000018 | C    | That is not a three :/  |
| .rdata:00444292 | 0000000F | C    | [*] Game over!  |
| .rdata:004442A4 | 00000044 | C    | [*] Next you will need to throw a one, press enter to throw a dice!                       |
| .rdata:004442E8 | 00000021 | C    | [*] You rolled a one! Very nice!  |
| .rdata:00444310 | 00000006 | C    | \a<0*0U   |
| .rdata:0044431E | 00000016 | C    | That is not a one :/  |
| .rdata:00444334 | 0000004C | C    | [*] Next you will need to throw another three, press enter to throw a dice!               |
| .rdata:00444380 | 00000021 | C    | [*] You rolled a three! Awesome!  |
| .rdata:004443A4 | 00000041 | C    | [*] Throw another three for me now, press enter to throw a dice!                          |
| .rdata:004443E8 | 00000030 | C    | [*] You rolled another three! Almost there now!   |
| .rdata:00444418 | 0000005C | C    | [*] The last character you need to roll is a seven.... (o_O) Press enter to throw a dice! |
| .rdata:00444474 | 00000045 | C    | [*] You rolled a seven, with a six sided dice! How awesome are you?!                      |
| .rdata:004444B9 | 00000018 | C    | That is not a seven :/  |
| .rdata:004444D1 | 00000006 | C    | ebCTF   |
| .rdata:004444D8 | 0000003E | C    | [*] You rolled 3-1-3-3-7, what does that make you? ELEET! \\o/                            |
| .rdata:00444518 | 00000021 | C    | [*] Nice job, here is the flag:   |
| .rdata:0044453C | 00000039 | C    | [!] It seems you did something wrong :( No flag for you.                                  |

通过这些字符串可以看到只有依次掷出3-1-3-3-7就有可能得到flag，但是要随机掷出这些数字明显不可能，因为其中有个7！为此，需要跟进字符串“[\*] You rolled a three! Good!”引用处查看程序的处理逻辑。

```

loc_401927:
cnp    [ebp+var_5C], 3
jnz    short loc_40198B

mov     dword ptr [esp+4], offset aYouRolledAThre ; "[*] You rolled a three! Good!"
mov     dword ptr [esp], offset __2St4cout ; int
mov     [ebp+var_120], 1
call   __2St1s1St11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; std::operator<<<std::char_1
mov     dword ptr [esp+4], offset __2St4endlcSt11char_traitsIcEERSt13basic_ostreamIT_T0_ES6_
mov     [esp], eax
call   __ZNSt13basic_ostreamIcT_E&#x2D;operator<<<(std::ostream & (*) (std::ostream &))
mov     dword ptr [esp+4], offset __2St4endlcSt11char_traitsIcEERSt13basic_ostreamIT_T0_ES6_
mov     [esp], eax
call   __ZNSt13basic_ostreamIcT_E&#x2D;operator<<<(std::ostream & (*) (std::ostream &))
mov     eax, [ebp+var_30]
add     eax, eax
mov     [ebp+var_30], eax
mov     dword ptr [esp+4], offset byte_444240 ; char *
lea     eax, [ebp+var_48]

```

从图中可以看到，程序通过判断[ebp+var\_5C]中的值是否为3进行跳转，如果为3则进入右边分支，程序继续执行；否则，程序跳转至loc\_40198B提示掷出的数字不是3，游戏结束！

```

loc_40198B:          ; "[*] You rolled a "
mov     dword ptr [esp+4], offset aYouRolledA
mov     dword ptr [esp], offset __ZSt4cout ; int
mov     [ebp+var_120], 1
call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_Pkc ; std::operator<<<std::char_traits<<
mov     edx, eax
mov     eax, [ebp+var_5C]
mov     [esp+4], eax
mov     [esp], edx
call    __ZNSolsEi ; std::ostream::operator<<(int)
mov     dword ptr [esp+4], offset aThatIsNotAThre ; " That is not a three :/"
mov     [esp], eax ; int
call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_Pkc ; std::operator<<<std::char_traits<<
mov     dword ptr [esp+4], offset __ZSt4endlIcSt11char_traitsIcEERSt13basic_ostreamIT_0_ES6_ ; std::
mov     [esp], eax
call    __ZNSolsEPFRSoS_E ; std::ostream::operator<<(std::ostream & (*) (std::ostream &))
mov     dword ptr [esp+4], offset aGameOver ; "[*] Game over!"
mov     dword ptr [esp], offset __ZSt4cout ; int
call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_Pkc ; std::operator<<<std::char_traits<<
mov     dword ptr [esp+4], offset __ZSt4endlIcSt11char_traitsIcEERSt13basic_ostreamIT_0_ES6_ ; std::
mov     [esp], eax
call    __ZNSolsEPFRSoS_E ; std::ostream::operator<<(std::ostream & (*) (std::ostream &))
lea     eax, [ebp+var_D8]
mov     [esp], eax ; this
mov     [ebp+var_120], 3
call    __ZNSsD1Ev ; std::string::~string()
lea     eax, [ebp+var_C8]
mov     [esp], eax ; this
mov     [ebp+var_120], 5
call    __ZNSsD1Ev ; std::string::~string()

```

80.00% (5052,14882) (14,9) 00000D8B 0040198B: WinMain(x,x,x,x):loc\_40198B

## 0x02 修改指令

理清程序的逻辑后，采用最简单的办法控制程序的执行路径——修改指令。首先，通过菜单栏中 Options/General/Disassembly/Number of opcode bytes 设置 IDA 使其显示指令的机器码。jnz 的机器码为 75，只需将其改为 jz 的机器码 74。修改方法：Edit/Patch program/Change byte。

通过 “[\*] You rolled a one! Very nice!” 等提示信息找到其他几处判断语句，使用相同的方法修改机器码。但是有两处为 near jump，jnz 的机器码为 0F 85，将其修改为 0F 84 即可。

修改完后 Edit/Patch program/Apply patches to input file 保存修改后的文件，运行便能得到 flag:ebCTF{64ec47ece868ba34a425d90044cd2dec}。

```

: 0 0 :
: 0 :
: 0 0 :
-----

[*] You rolled another three! Almost there now!

[*] The last character you need to roll is a seven.... (o_0) Press enter to th
row a dice!

-----

: 0 0 :
: 0 :
: 0 0 :
-----

[*] You rolled a seven, with a six sided dice! How awesome are you?!

[*] You rolled 3-1-3-3-7, what does that make you? ELEET! \o/
[*] Nice job, here is the flag: ebCTF{64ec47ece868ba34a425d90044cd2dec}

```