南開大學

汇编语言与逆向技术课程实验报告

实验十：CaptureTheFlag

学　　院　网络空间安全学院

专　　业　信息安全

学　　号　2313546

姓　　名　蒋枘言

班　　级　信息安全班

一、实验目的

1.熟悉静态反汇编工具 Binary Ninja；

2.掌握对二进制代码内部逻辑关系的分析；

3.掌握对二进制代码的修改和保存。

二、逆向分析

（一）主要结构

游戏一共有 4 个关卡，每通关一关，KEY 的值就会加 1，进度增加 25%。

```
004eb478  char const data_4eb478[0x20] = "Z KEY DECRYPTING PROGRESS : 0%%", 0
004eb498  char const data_4eb498[0x21] = "Z KEY DECRYPTING PROGRESS : 25%%", 0

004eb4b9                              00 00 00                          ...

004eb4bc  char const data_4eb4bc[0x21] = "Z KEY DECRYPTING PROGRESS : 50%%", 0

004eb4dd                                          00 00 00                  ...

004eb4e0  char const data_4eb4e0[0x21] = "Z KEY DECRYPTING PROGRESS : 75%%", 0
```

```
004e0004  _.data:
004e0004                  08 90 f6 1a-e3 0e 23 46 af 07 84 59
004e0010  89 3e f0 59
004e0014  KEY::v2:
004e0014                  0b 4c 30 05-d8 29 25 05 5a e6 c6 4c
004e0020  3e bb f6 7c
004e0024  KEY::v3:
004e0024                  08 fd 07 a6-67 92 a1 39 cd 0d 28 ea
004e0030  95 0c e0 aa
004e0034  KEY::v4:
004e0034                  e5 d3 8f 7b-f5 cb 69 6f c8 53 44 39
004e0040  43 55 5d 60
004e0044  char KEY::n[0x0] =
004e0044  {
004e0044  }
004e0044                  04 00 00 00
```

（二）重要数据

_MOVE_SPEED：主角移动速度

_MAX_HP：最大血量

_ARMOR：防御值

_FIRE_SPEED：初始血量

_INITIAL_HP：子弹速度

```
004e0048  int32_t _MOVE_SPEED = 0x40490fda
004e004c  int32_t _MAX_HP = 0x43960000
004e0050  int32_t _ARMOR = 0x41200000
004e0054  int32_t _spawnX = 0x41200000
004e0058  int32_t _spawnY = 0x43960000
004e005c  int32_t _csize_x = 0x42000000
004e0060  int32_t _csize_y = 0x42400000
004e0064  int32_t _last_combat = -0x64
004e0068  int32_t _FIRE_SPEED = 0x41000000
004e006c  int32_t _FIRE_SCOPE = 0x49435000
004e0070  int32_t _INITIAL_HP = 0x43960000
004e0074  int32_t _SLOW_DEG = 0x3f800000
004e0078  int32_t _cur_map = 0x1
004e007c  int32_t _weapon_index = 0x1
004e0080  int32_t _weapons_total = 0x4
004e0084  int32_t _weapons_now = 0x1
004e0088  int32_t _cur_weapon = 0x2
004e008c  int32_t _.data = 0x100
004e0090  int32_t ege::g_windowpos_y = -0x80000000
004e0094  int32_t ege::g_windowpos_x = -0x80000000
004e0098  int32_t ege::g_windowstyle = 0x12ca0000
004e009c  int32_t _.data = 0x400
```

三、修改静态资源与反汇编指令

（一）修改静态资源

在一开始，我们发现主角移动速度非常慢，而且血条有限，非常容易就死了。于是，我们修改一些静态资源：

~~将_MOVE_SPEED 修改为 0x40fffff。~~（不能修改速度，好像修改了有的桥就过不去了？）

将_MAX_HP 修改为 0x7f960000。

将_FIRE_SCOPE 修改为 0x0。

将_INITIAL_HP 修改为 0x7F960000。

将_MAX_HP 修改为 0x。

```
004e0000  0a 00 00 00 08 90 f6 1a-e3 0e 23 46 af 07 84 59-89 3e f0 59 0b 4c 30 05-d8 29 25 05 5a e6 c6 4c
004e0020  3e bb f6 7c 08 fd 07 a6-67 92 a1 39 cd 0d 28 ea-95 0c e0 aa e5 d3 8f 7b-f5 cb 69 6f c8 53 44 39
004e0040  43 55 5d 60 04 00 00 00-ff ff ff 40 00 00 96 7f-00 00 20 41 00 00 20 41-00 00 96 43 00 00 00 42
004e0060  00 00 40 42 9c ff ff ff-00 00 00 41 00 50 43 49-00 00 96 43 00 00 80 3f-01 00 00 00 01 00 00 00
004e0080  04 00 00 00 01 00 00 00-02 00 00 00 00 01 00 00-00 00 00 80 00 00 00 80-00 00 ca 12 00 04 00 00
```

于是这个时候就无敌了，不会死掉。

但是这些敌人还是非常难消灭，并且运用一次大招非常消耗钻石。我们可以把大招消耗的钻石数改为 0。

根据字符串“This skill needs XXX MP!”，找到数据位置。

```
00407eab  a188004e00          mov     eax, dword [_cur_weapon]
00407eb0  8b048540dd4f00      mov     eax, dword [eax*4+0x4fdd40]
00407eb7  89442408            mov     dword [esp+0x8 {var_2a4_9}], eax
00407ebb  c744240450b54e00    mov     dword [esp+0x4 {_Format_2}], data_4eb550  {"This skill needs %d MP!"}
00407ec3  8d85f0fdffff        lea     eax, [ebp-0x210 {var_214}]
00407ec9  890424              mov     dword [esp {var_2ac}], eax {var_214}
00407ecc  e8bfbd0600          call    sprintf
00407ed1  c744240441000000    mov     dword [esp+0x4 {var_2a8_20}], 0x41
```

```
00406638  c70548dd4f000000…  mov     dword [data_4fdd48], 0x0
00406642  c7054cdd4f000500…  mov     dword [data_4fdd4c], 0x5
0040664c  c70550dd4f000a00…  mov     dword [data_4fdd50], 0xa
```

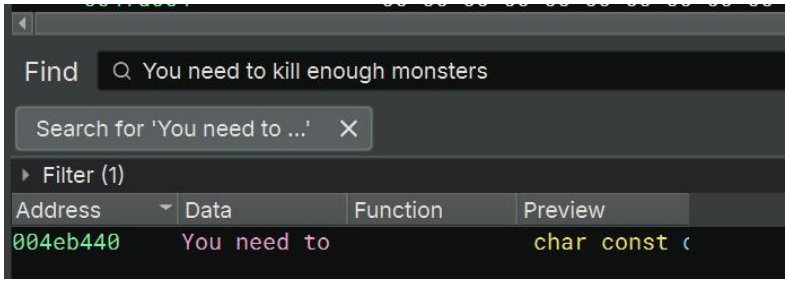
```
00406638  c70548dd4f000000…  mov     dword [data_4fdd48], 0x0
00406642  c7054cdd4f000000…  mov     dword [data_4fdd4c], 0x0
0040664c  c70550dd4f000000…  mov     dword [data_4fdd50], 0x0
```

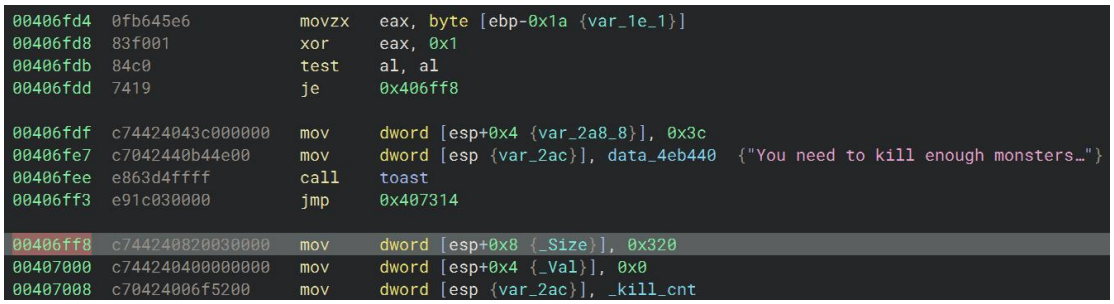
把这些全改为 0 之后，就可以无限放大招了。

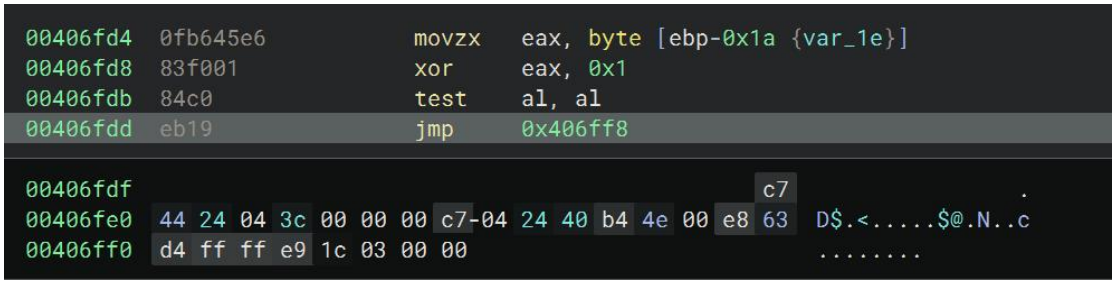
（二）修改反汇编指令

前三关现在直接打完全可以通过，但是第四关会出现卡关的情况，把仅有的怪打死之后，还是会提示“You need to kill enough monsters!”。此时需要修改反汇编指令。

根据字符串“You need to kill enough monsters!”，找到指令位置，把相等才跳转 je 改成 jmp 无条件跳转即可。







四、重新游戏并通关

重新开始游戏，于是成功通关。通关的截图如下：

得到 flag 为 a2fdkd80xo。