

Lab7 - Game/CTF (Capture The Flag) 夺旗赛

一、实验目的

- ## 二、实验原理

三、三：实验内容

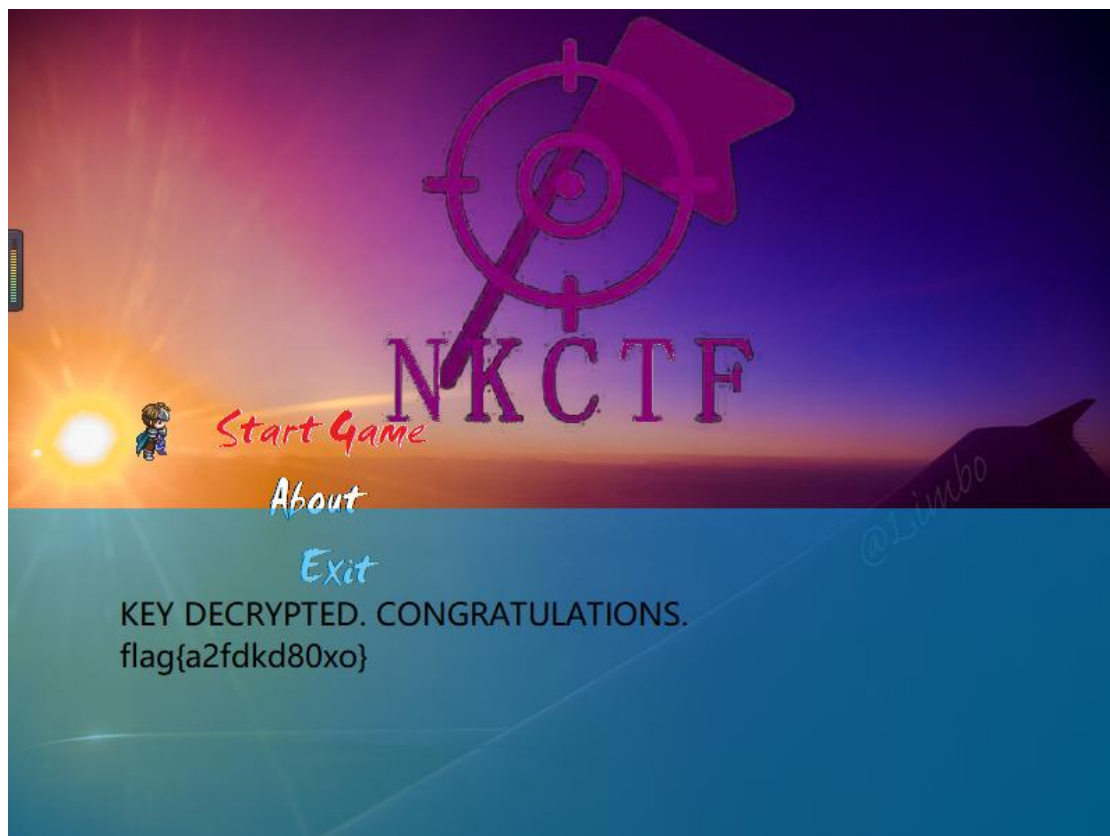
-
- IDA Pro interface showing the Hex View of a binary file. The left pane displays the C source code for a function named 'tf'. The right pane shows the corresponding assembly code in hex view, with various instructions and data segments visible. The status bar at the bottom indicates the current address is 16.77% (7275.22403) and the function is 'mainloop(void):loc_408FB1'.

```

.data:004E0042 db 5Dh ; J
.data:004E0043 db 60h ; ~
.data:004E0044 public __ZN3KEY1nE
.data:004E0044 ; KEY::n
.data:004E0044 __ZN3KEY1nE dd 4 ; DATA XREF: KEY::writekey(int):loc_403DC2↑r
.data:004E0048 public _MOVE_SPEED
.data:004E0048 _MOVE_SPEED dd 3.1415925 ; DATA XREF: mainloop(void)+12B7↑r
; mainloop(void)+12D6↑r ...
; 移动速度
.data:004E004C public _MAX_HP
.data:004E004C _MAX_HP dd 43960000h ; DATA XREF: save(savedata &)+18↑r
; apply_save(savedata)+1E↑w ...
; 血量
.data:004E0050 public _ARMOR
.data:004E0050 _ARMOR dd 41200000h ; DATA XREF: save(savedata &)+4A↑r
; apply_save(savedata)+44↑w ...
.data:004E0054 public _spawnX
.data:004E0054 ; float spawnX
.data:004E0054 _spawnX dd 41200000h ; DATA XREF: logic_init(void)+A5↑r
; mainloop(void)+5DC↑w
.data:004E0058 public _spawnY
.data:004E0058 ; float spawnY
.data:004E0058 _spawnY dd 43960000h ; DATA XREF: logic_init(void)+9F↑r
; mainloop(void)+5FF↑w
.data:004F0058
00000048 0000000000004E0048: .data: _MOVE_SPEED (Synchronized with Rev View-1)

```

2. 修改 game.exe 二进制代码，获得最后的 Flag。实验报告要说明逆向分析、代码修改的具体过程，以及最后获得的 Flag。



1. 进入游戏，人物生命值极有限，_MAX_HP,_INITIAL_HP 改为无限，如下：

在十六进制视图中（Hex View）找到指定区域，右键选择 Edit 对资源进行修改。修改完毕后，右键选择 Apply changes 应用修改

点击 Edit->Patch program->Apply patches to input file

```
.data:004E004C      public _MAX_HP
.data:004E004C      _MAX_HP      dd 7FFFFFFFh          ; DATA XREF: save(savedata &)+18↑r
.data:004E004C      ; apply_save(savedata)+1E↑w ...

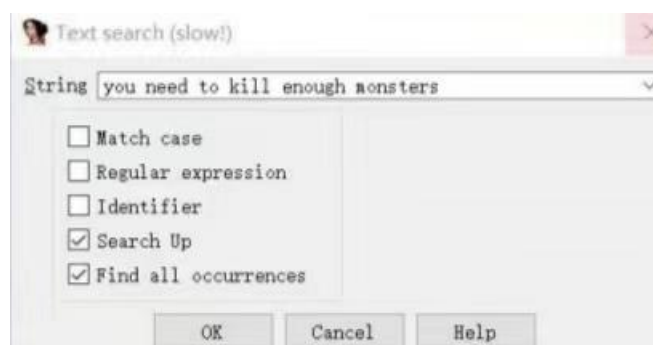
.data:004E0070      public _INITIAL_HP
.data:004E0070      _INITIAL_HP    dd 7FFFFFFFh          ; DATA XREF: data_init(void)+6↑r
.data:004E0074      ; ...
```

2. 要想从第二个界面进入第三个界面，发现 “You need to kill enough monsters” ,修改

在反汇编代码中（IDA View）找到需要修改的汇编指令

点击 Edit->Patch program->Assemble，输入新的汇编指令

点击 Edit->Patch program->Apply patches to input file



```
.text:00406FD4      movzx  eax, [ebp+var_1A]
.text:00406FD8      xor    eax, 1
.text:00406FDB      test   al, al
.text:00406FDD      jmp    short loc_406FF8
.text:00406FDF      ;
.text:00406FDF      mov    dword ptr [esp+4], 3Ch ; '<' ; int
.text:00406FE7      mov    dword ptr [esp], offset Str ; "You need to kill enough monsters!"
.text:00406FEE      call   __Z5toastPci ; toast(char *,int)
.text:00406FF3      jmp    loc_407314
.text:00406FF8      ;
```

3. 按照地图指示和人物对话信息可通关，得 Flag

