<参考答案见视频源码下载>

1、使用CE软件 搜索任意一款软件 找到某个基址，并在CE中修改这个值。(CE见附件)

2、画出下面程序的堆栈图，找到局部变量在哪里？

int plus(int x,int y)

{

int a;

int b;

int z;

z = a+b+x+y;

return z;

}

void main() //入口程序 程序开始执行的地方

{

plus(1,2);

return; //执行结束

}

压栈参数,函数调用,外平栈

00401078 push 2

0040107A push 1

0040107C call @ILT+0(plus) (00401005)

00401081 add esp,8

中转

00401005 jmp plus (00401020)

压栈ebp,提升ebp,提升esp,压栈ebx/esi/edi/,循环填充ebp-4Ch

00401020 push ebp

00401021 mov ebp,esp

00401023 sub esp,4Ch

00401026 push ebx

00401027 push esi

00401028 push edi

00401029 lea edi,[ebp-4Ch]

0040102C mov ecx,13h

00401031 mov eax,0CCCCCCCCh

00401036 rep stos dword ptr [edi]

4: int a;

5: int b;

6: int z;

7: z = a+b+x+y;

00401038 mov eax,dword ptr [ebp-4]

0040103B add eax,dword ptr [ebp-8]

0040103E add eax,dword ptr [ebp+8]

00401041 add eax,dword ptr [ebp+0Ch]

00401044 mov dword ptr [ebp-0Ch],eax

8: return z;

00401047 mov eax,dword ptr [ebp-0Ch]

出栈edi/esi/ebx,还原esp,还原ebp,函数返回

0040104A pop edi

0040104B pop esi

0040104C pop ebx

0040104D mov esp,ebp

0040104F pop ebp

00401050 ret

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  | edi | esp:0018FE94 | | edi |  |
|  |  |  | esi |  |  | esi |  |
|  |  |  | ebx |  |  | ebx |  |
|  |  |  | CCCCCCCC | esp:0018FEA0 | | CCCCCCCC |  |
|  |  |  | CCCCCCCC |  |  | CCCCCCCC |  |
|  |  |  | CCCCCCCC |  |  | CCCCCCCC |  |
|  |  |  | CCCCCCCC |  |  | CCCCCCCC |  |
|  |  |  | CCCCCCCC |  |  | CCCCCCCC |  |
|  |  |  | CCCCCCCC | 局部变量a,b | | CCCCCCCC |  |
|  |  |  | 0018FF48 | ebp:0018FEEC | | 0018FF48 |  |
| 00401081 | esp:0018FEF0 | | 00401081 | esp:0018FEF0 | | 00401081 |  |
| 1 | esp:0018FEF4 | | 1 | esp:0018FEF4 | | 1 |  |
| 2 |  |  | 2 |  |  | 2 |  |
|  | esp:0018FEFC | |  | esp:0018FEFC | |  | esp:0018FEFC |
|  |  |  |  |  |  |  |  |
|  | ebp:0018FF48 | |  | ebp:0018FF48 | |  | ebp:0018FF48 |
| 压栈参数,函数调用 | |  | 压栈ebp,提升ebp | |  | 出栈edi,esi,ebx | |
|  |  |  | 提升esp压栈ebx,esi,edi | | | 还原esp,还原ebp | |
|  |  |  | 循环填充ebp-4Ch | |  | 函数返回,外平栈 | |

3、局部变量在使用前必须要赋值，请说明为什么？

因为内存是重复被使用的不赋初值的话可能有垃圾数据或填充数据被调用造成错误