C++ Tricks 2.3 I386[illegible]C[illegible]

[illegible] farseerfc.wordpress.com [illegible]

2.3 I386[illegible]C[illegible]

[illegible]esp[illegible]esp[illegible]

[illegible]esp[illegible]esp[illegible]esp[illegible]ebp[illegible]ebp[illegible]ebp[illegible]

void f()

{

int a=0; //a□□□□□□□ebp-4

char c=1; //c□□□□□□□ebp-8

}

□□□□□□□□□

push ebp ;□ebp□□

mov ebp,esp ;ebp=esp □□□□□□□□□

sub esp,8 ;esp-=8□□a□c□□□□□□□□□□

mov dword ptr[ebp-4],0 ;a=0

mov byte ptr[ebp-8],1 ;c=1

add esp,8 ;esp+=8□□□a□c□□□

mov esp,ebp ;esp=ebp □□□□□□□□

pop ebp ;□□ebp

ret ;□□

□□□□□□□□□□

09992:c=1 <-esp

09996:a=0

10000:□ebp <-ebp

10004:……

□:□□□□pop□push□call□ret□□□□□□□□□□□□□□□□□□□□□□□□

push ebp□□□:

add esp,4

mov dword ptr[esp],ebp

pop ebp□□□□

mov ebp,dword ptr[esp]

sub esp,4

call fun_address[illegible]

push eip

jmp fun_address

ret[illegible]

add esp,4

jmp dword ptr[esp-4]

[illegible]ret

ret 8[illegible]

add esp,12

jmp dword ptr[esp-4]

[illegible]

void f()

{

int i,a[10];

for(i=0;i<=10;++i)a[i]=0;/An error occurs here!

}

[illegible]C++[illegible]“[illegible]”[illegible]

[illegible]a[10][illegible]a[10][illegible]C++[illegible]“[illegible]”[illegible]a[10][illegible]a[illegible]i!

[illegible]i[illegible]a[illegible]a[illegible]I386[illegible]a[illegible]i[illegible]a[i][illegible]i[illegible]a[i][illegible]i[illegible]0[illegible]

[illegible]……[illegible]
[illegible]……[illegible]Kill[illegible]……