《软件安全》实验报告

姓名:曹瑜 学号: 2212794 班级: 密码科学与技术

实验名称:

Shellcode 编写及编码实验

实验要求:

复现第五章实验三,并将产生的编码后的 shellcode 在示例 5-4 中进行验证,阐述 shellcode 编码的原理, shellcode 提取的思想

实验过程:

讲入 VC:



进入 VC 反汇编可见代码逻辑:

```
shellcode - Microsoft Visual C++ [break] - [Disassembly]
文件(E) 編輯(E) 查看(Y) 插入(E) 工程(P) 调试(B) 工具(E) 窗口(E) 帮助(B)
(Globals) (All global members → main
                                                                                                shellcode wWin32 Debug
                                                                                                                                                                       - K- 8 M - 1 H 0
                                                                                                                                              # # # P P P P P B B B B B B B
                                    4: {
00401010
00401011
00401013
■ 工作区 'shellcode': 1 

■ shellcode files
■ Source Files
■ Header Files
                                                   push
push
push
lea
                                    00401016
                                    00401017
                                09461917
09461919
09461919
09461912
09461921
09461926
55:
◆ 09461928
09461926
09461926
09461938
09461938
       Resource Files
                                                                    edi
edi,[ebp-40h]
ecx,10h
eax,0cccccccch
    External Depend
                                                  rep stos dword ptr [edi]
MessageBox(NULL,NULL,NULL,0);
                                                   mov
push
push
push
push
call
                                                                    u
dword ptr [_imp_MessageBoxA@16 (0042a2ac)]
esi,esp
__chkesp (00401070)
                                    00401038
0040103A
                                                  return;
```

```
#include <stdio.h>
#include <windows.h>
void main()
{|
    _asm{
    xor ebx,ebx
    push ebx//push 0
    push ebx
    push ebx
    push ebx
    push ebx
    mov eax, 77d507eah// 77d507eah 这个是 MessageBox 函数在系统中的地址
    call eax
    }
    return;
}
```

转到起始句反汇编

```
#include <stdio.h>
#include <windows.h>
void main()
{
    _asm{
        xor ebx,ebx
        push ebx//push 0
        push ebx
        push ebx
        push ebx
        push ebx
        push ebx
        cor eax, 77d507eah// 77d507eah 这个是 MessageBox 函数在系统中的地址
        call eax
        }
        return;
}
```

```
© 00401028
                        ebx,ebx
            xor
           push ebx//push 0
  7:
  0040102A
            push
                        ebx
  8:
           push ebx
  0040102B
            push
                        ebx
  9:
           push ebx
  0040102C
            push
                        ebx
           push ebx
  10:
  0040102D
                        ebx
            push
             mov eax, 77d507eah// 77d507eah 这个是 MessageBox 函数在系统中的地址
  11:
  0040102E
                        eax,77D507EAh
            mnu
  12:
           call eax
  00401033
            call
                        eax
  13:
  14:
  15:
           return;
  16:
  00401035
                        edi
            pop
```

转到对应区域地址,可见该部分指令从地址 00401028 到 00401034 处

根据地址可定位到对应的机器码

新建文本存储对应机器码

```
    新建 文本文档.txt - 记事本

    文件(P) 編辑(B) 格式(D) 查看(V) 帮助(H)

    33 DB 53 53 53 53 B8 EA 07 D5 77 FF D0
```

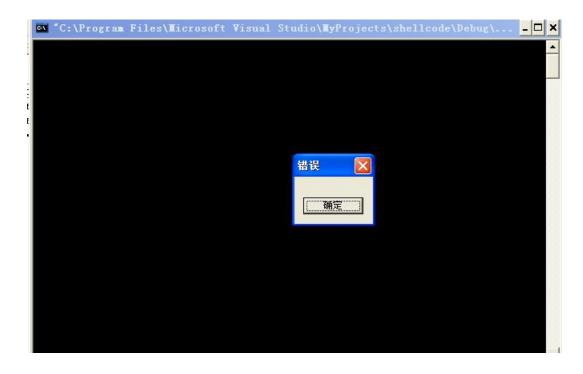
利用该 shellcode 实现漏洞利用,编写调试程序验证:

```
#include <stdio.h>
#include <windows.h>
char ourshellcode[]="\x33\xDB\x53\x53\x53\x53\x53\x53\x53\x55\x77\xFF\xD6";
void main()
{
    LoadLibrary("user32.dll");
    int *ret;
    ret=(int*)&ret+2;
    (*ret)=(int)ourshellcode;
    return;
}ss
```

处理所得机器码

```
新建文本文档.txt - 记事本
文件(P) 編輯(E) 格式(E) 查看(Y) 帮助(E)
\x33\xDB\x53\x53\x53\x53\x53\xB8\xEA\x07\xD5\x77\xFF\xD0
```

运行程序可得知该 shellcode 可以调用 MessageBox



```
C:\Program Files\Licrosoft Visual Studio\LyProjects\shellcode\Debug\... - X

Press any key to continue...
```

心得体会:

通过本次实验,掌握了如何根据汇编代码,找到对应地址的机器码,对 shellcode 进行编码和解码操作。通过本次实验,基于理论知识的学习初次尝试了 shellcode 的提取和调试,对 shellcode 的提取和编译有了更深入的了解。