第十一章 Hook入门

北京邮电大学
崔宝江

第十一章 Hook入门

- 一. Hook概述
- 二. API Hook
- 三.逆向分析

北邮网安学院　崔宝江

一. Hook概述

- 1 Hook概念及其种类
- 2 Message Hook
- 3 IAT Hook

一. Hook概述

- Hook概念及其种类
  - 中文名叫做“钩子”或者“钩取”
  - hook技术能在程序实现正常功能的情况下，获取到程序的目的参数，信息等，或者实现嵌入的代码功能
  - 应用程序的补丁，程序的破解，插件的开发等等，都可能需要通过hook来实现
  - 可以进行钩取的方法有很多
    - 在Windows中，hook的方法主要有Message Hook，IAT Hook，API Hook等等，本章将重点讲解API Hook。

一. Hook概述

- 2 Message Hook
  - Message Hook也叫做消息钩子，针对的是GUI（图形用户界面）程序
  - 使用的关键Windows API函数SetWindowsHookEx，MSDN(Microsoft Developer Network)定义如下

```
HHOOK WINAPI SetWindowsHookEx(
  _In_ int       idHook,
  _In_ HOOKPROC  lpfn,
  _In_ HINSTANCE hMod,
  _In_ DWORD     dwThreadId
);
```


一. Hook概述

- 第一个参数是windows 消息值
  - 比如WH_KEYBOARD可以控制WM_KEYUP和WM_KEYDOWN两个消息值（是描述键盘虚拟键码的，它对应的是键盘物理按键Pgup和Pgdn）
- 第二个参数是我们对应消息的回调函数
  - 比如当触发按键消息的时候，设置的对应按键回调函数就会调用。
- 第三个参数是包含hook代码的动态链接库DLL句柄
- 第四个参数是所钩取的线程id，如果设置为0，则为全局钩取，即所有的GUI程序都将被钩取。

```
HHOOK WINAPI SetWindowsHookEx(
  _In_ int       idHook,
  _In_ HOOKPROC  lpfn,
  _In_ HINSTANCE hMod,
  _In_ DWORD     dwThreadId
);
```

一. Hook概述

- 在使用**SetWindowsHookEx**函数以后，消息钩子会先于应用程序看到相应的消息，并对消息进行拦截，处理，调用回调函数里的代码。

一. Hook概述

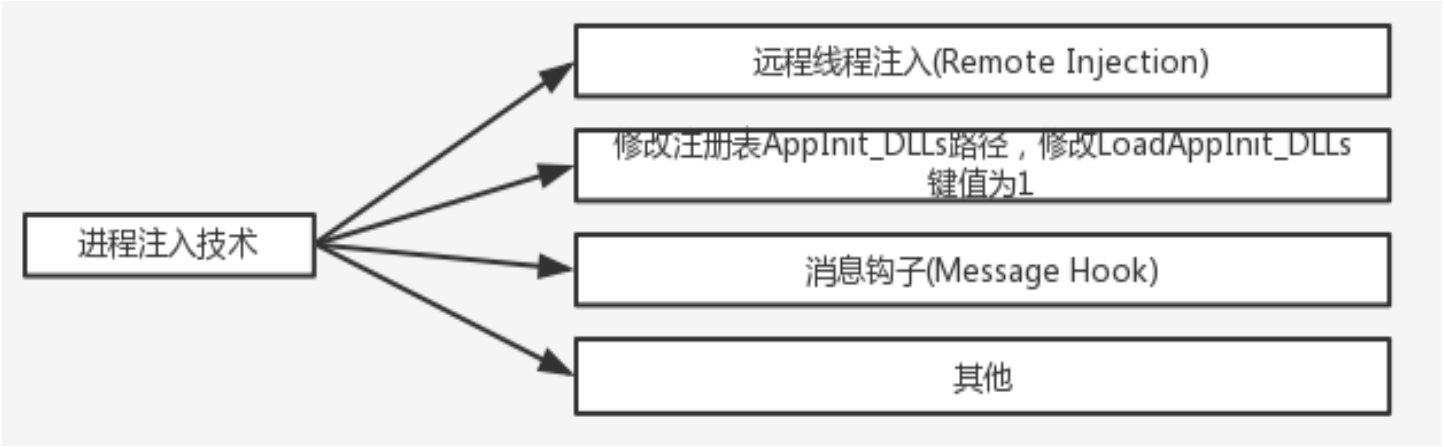
- 自己写的回调函数代码应该是在我们自己写的应用程序里，怎么会被其他应用程序调用的呢，进程和进程之间不应该是相互隔离的么？
- 在**SetWindowsHookEx**函数成功产生作用时，对应监控的应用程序里会被注入一个动态链接库**DLL**，我们的关键代码就写在被加载的这个**DLL**当中
- 下面简单介绍一下进程注入

一. Hook概述

- 进程注入需求的产生
  - 应用程序之间是相互独立的，各自享有自己的内存空间
  - 应用程序需要跨越进程边界来访问另一个进程的地址空间时，就会使用进程注入。
  - 为了对内存中的某个进程进行操作，并且获得该进程地址空间里的数据，或者修改进程的私有数据，修改程序执行流，就需要把代码放入到目的进程当中，这时就避免不了使用进程注入方法了。

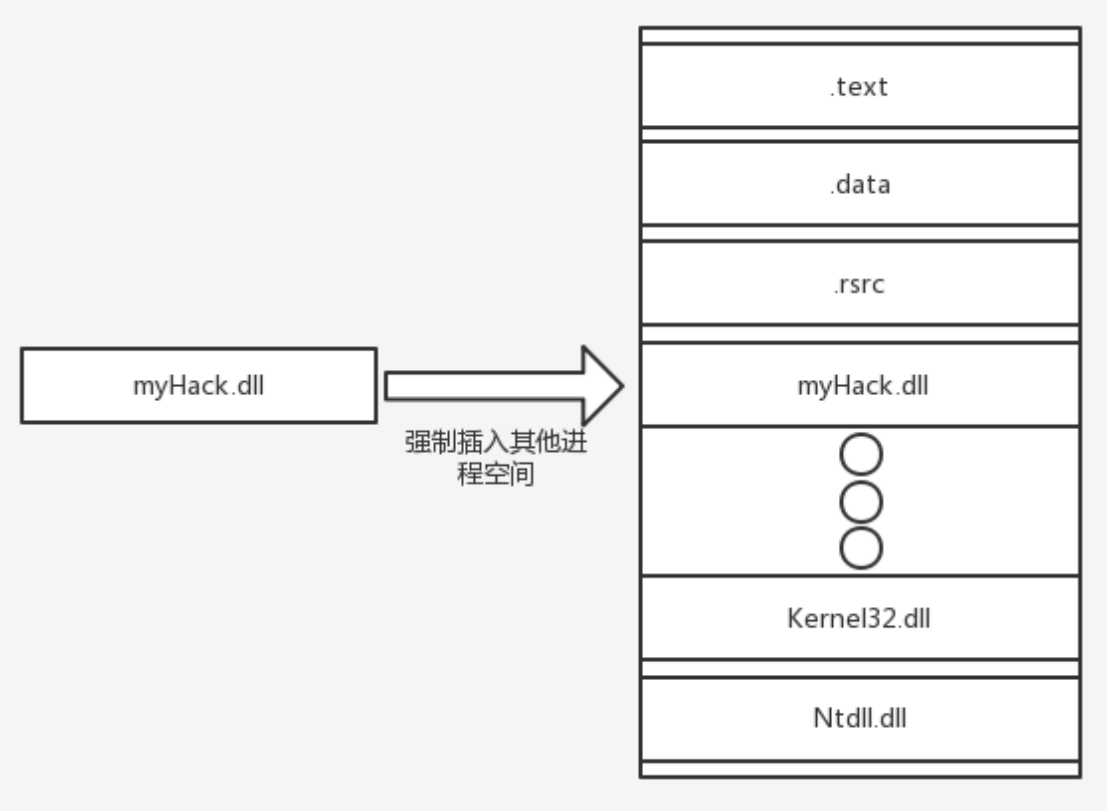
一. Hook概述

- 进程注入的方法有很多



一. Hook概述

- 进程注入图示



一. Hook概述

- Message Hook方式虽然简单，但是也存在不足，它只能捕获Windows操作系统向用户提供的消息事件，诸如借助键盘，鼠标操作的事件，能够控制的函数有限
  - 具体的消息范围都可以在MSDN的介绍中找到

一. Hook概述

- 3 IAT Hook
  - 对于32位的PE程序来讲，结构中有一个IMPORT Table，IMPORT Table包含两个元素
    - 一个是第一个IMAGE_IMPORT_DESCRIPTOR的起始地址，另一个元素则是整个IMPORT Table的大小。
  - IMPORT Table中又有多个IMAGE_IMPORT_DESCRIPTOR（IDT）
    - 其中一个IDT的大小是20字节，一个空的20字节作为末尾
  - 用IMPORT Table的大小除以20，再减去1，就可以得到IDT的数量。

一. Hook概述

- IDT包含的结构如图
  - 观察PE结构所使用的工具是PEView

VA	Data	Description	Value
00403394	000033D0	Import Name Table RVA	
00403398	00000000	Time Date Stamp	
0040339C	00000000	Forwarder Chain	
004033A0	00003560	Name RVA	KERNEL32.dll
004033A4	00003000	Import Address Table RVA	
004033A8	0000341C	Import Name Table RVA	
004033AC	00000000	Time Date Stamp	
004033B0	00000000	Forwarder Chain	
004033B4	000035C8	Name RVA	MSVCR110.dll
004033B8	0000304C	Import Address Table RVA	
004033BC	00000000		
004033C0	00000000		
004033C4	00000000		
004033C8	00000000		
004033CC	00000000		

一. Hook概述

- 在程序没有加载的时候，**Import Address Table**中的值和**Import Name Table** 的值一样，都是指向导入函数的名称。
- 当程序动态加载以后，装载器在每一个动态链接库加载过程中，都会把实际的函数地址填入**Import Address Table**当中，这样我们的程序在运行的过程中就可以直接调用了。

一. Hook概述

- IAT Hook原理
  - 在程序动态装载以后，先获得原始目标API的函数地址，然后保存在一个变量里。
  - 通过查找IAT的形式，找到IAT表。
  - 将IAT中的每一项的值和之前保存目标API函数地址的变量值进行比较，如果相同，则替换成我们自己函数的地址。

一. Hook概述

- IAT Hook方式也存在局限性
  - IAT Hook需要在程序动态装载以后，才能实施将hook程序装载进的API函数地址
  - 如果需要hook的某个函数并没有动态加载，那么这种思路行不通

第十一章 Hook入门

- 一. Hook概述
- 二. API Hook
- 三.逆向分析

北邮网安学院　崔宝江

二. API Hook

- 1 API Hook原理
- 2 动态调试API Hook

二. API Hook

- **API**
  - **Application Programming Interface**，应用程序编程接口
  - **Windows API**是一个实现某种功能的函数，一个内部已经封装好代码的函数，用户在使用时，无需知道其内部实现，或是理解它与系统的软硬件是如何交互的，只需要明白该**API**函数如何使用，通过这个接口来实现某种特定功能，这就是**API**。

二. API Hook

- 标准的API Hook的实现步骤
  - 第一步，获取API的函数地址
  - 第二步，修改API起始地址字节，使之跳转到我们自己定义的函数
  - 第三步，在自定义的函数中实现unhook（脱钩），恢复原API起始地址处字节
  - 第四步，执行我们自定义的代码以及原API函数，再次hook该API函数，便于下次拦截，最后返回

二. API Hook

- 第一步，获取API函数的地址
  - 例子：获取WriteFile函数地址。

```
#include<stdio.h>
#include<Windows.h>
Int main()
{
        HMODULE hKernel32;
        FARPROC pWriteFile;
        hKernel32 =GetModuleHandle(L"kernel32.dll");
        pWriteFile=GetProcAddress(hKernel32, "WriteFile");
        printf("0x%p\n", pWriteFile);
Return 0;
}
```

  - 相关Windows API使用可搜索msdn

二. API Hook

- 第二步，修改API函数起始地址处字节
  - 以x86为例
  - hook的原理是相同的，但是处理细节确是不同的
    - 以Ke，Nt，Zw开头的API，以及32位和64位系统下的API函数地址，入口处可修改的字节码数量可能是不同的，在处理时的细节上可能有所差异，
    - 没有一成不变的hook模板。需要用户在hook之前，自行调试，确认修改的字节无误。

```
#include<stdio.h>
#include<windows.h>
BYTE pOrgByte[5] = { 0, };
Typedef BOOL(WINAPI *PFWriteFile)(HANDLE hFile, LPCVOID lpBuffer, DWORD nNumberOfBytesToWrite, LPDWORD
lpNumberOfBytesWritten, LPOVERLAPPED lpOverlapped);
Void unhook()
{
}
BOOL MyWriteFile(HANDLE hFile, LPCVOID lpBuffer, DWORD nNumberOfBytesToWrite, LPDWORD lpNumberOfBytesWritten,
LPOVERLAPPED lpOverlapped)
{
        FARPROC pFunc;
        unhook();
        pFunc=GetProcAddress(GetModuleHandleA("kernel32.dll"), "WriteFile");
        ((PFWriteFile)pFunc)(hFile, lpBuffer, nNumberOfBytesToWrite, lpNumberOfBytesWritten, lpOverlapped);
        return TRUE;
}
Int main()
{
        HMODULE hKernel32;
        FARPROC pWriteFile;
        PBYTE pEditFunc;
        byte pJmpCode[6] = { 0xE9,0, };
        DWORD dwOldProtect,pOffset;
        hKernel32 =GetModuleHandle(L"kernel32.dll");
        pWriteFile=GetProcAddress(hKernel32, "WriteFile");
        pEditFunc= (PBYTE)pWriteFile;
        if (VirtualProtect(pEditFunc, 5, PAGE_EXECUTE_READWRITE, &dwOldProtect))
        {
                memcpy(pOrgByte, pEditFunc, 5);
                pOffset= (ULONGLONG)MyWriteFile- (ULONGLONG)pWriteFile-5;
                memcpy(&pJmpCode[1], &pOffset, 4);
                memcpy(pWriteFile, &pJmpCode[0], 5);
                VirtualProtect(pWriteFile, 5, dwOldProtect, &dwOldProtect);
        }
return0;
}
```

二. API Hook

- 重点是main函数中的VirtualProtect函数
  - VirtualProtect能够改变指定地址处，指定字节数量的可读可写可执行属性。
    1. 获取WriteFile的地址
    2. 对WriteFile地址处的5个字节修改了属性，使该5个字节可读、可写、可执行
    3. 保存原始WriteFile函数的5个字节
    4. 获得我们的自定义函数MyWriteFile和WriteFile函数间的偏移，保存于变量pOffset当中
    5. 之后两次memcpy函数的调用修改了WriteFile起始地址处的5个字节
    6. 最后，恢复WriteFile函数处的代码属性

二. API Hook

- 0xE9是Jmp指令的字节码，其后跟随4个将会被解析为跳转偏移的字节码，这样一来，当我们调用WriteFile函数的时候，就会跳转到MyWriteFile执行。

二. API Hook

- 第三步，在自定义的函数中实现**unhook**（脱钩），恢复原**API**起始地址处字节。
  - 第二步中，**MyWriteFile**函数中的**unhook**即是我们的脱钩函数
  - 脱钩函数在自定义函数中并不是必须存在的，如果不调用原来系统本身的**API**，可以选择不对函数进行脱钩，直接执行我们自己的代码。
  - 注意：我们自定义的函数，函数的返回值，参数类型，参数个数要与被**hook**的**API**保持一致，目的是保证程序在运行过程中的堆栈平衡。

二. API Hook

```
#include<stdio.h>
#include<Windows.h>
BYTE pOrgByte[6] = { 0, };
Void unhook()
{
        DWORD dwOldProtect;
        PBYTE pWriteFile;
        FARPROC pFunc;
        pFunc=GetProcAddress(GetModuleHandleA("kernel32.dll"), "WriteFile");
        pWriteFile= (PBYTE)pFunc;
        VirtualProtect(pWriteFile, 5, PAGE_EXECUTE_READWRITE, &dwOldProtect);
        memcpy(pWriteFile, pOrgByte, 5);
        VirtualProtect(pWriteFile, 5, dwOldProtect, &dwOldProtect);
}
intmain()
{
        unhook();
return0;
}
```


二. API Hook

- 上述代码unhook函数用于脱钩
  - 使用VirtualProtect函数，先将已经修改掉的WriteFile函数地址处5字节修改代码属性
  - 然后将原WriteFile的5个字节copy回去，其中pOrgByte是之前hook代码时，保存的原WriteFile函数地址处5个字节的变量。

二. API Hook

- 第四步，执行我们自定义的代码以及原API函数，再次hook该API函数，便于下次拦截，最后返回。
- 执行了我们自己的代码以后，需不需要再次hook住该API函数，是由我们自己决定的。如果我们只选择进行一次hook，那么在unhook以及执行完我们自己的代码以后，就可以直接返回了。

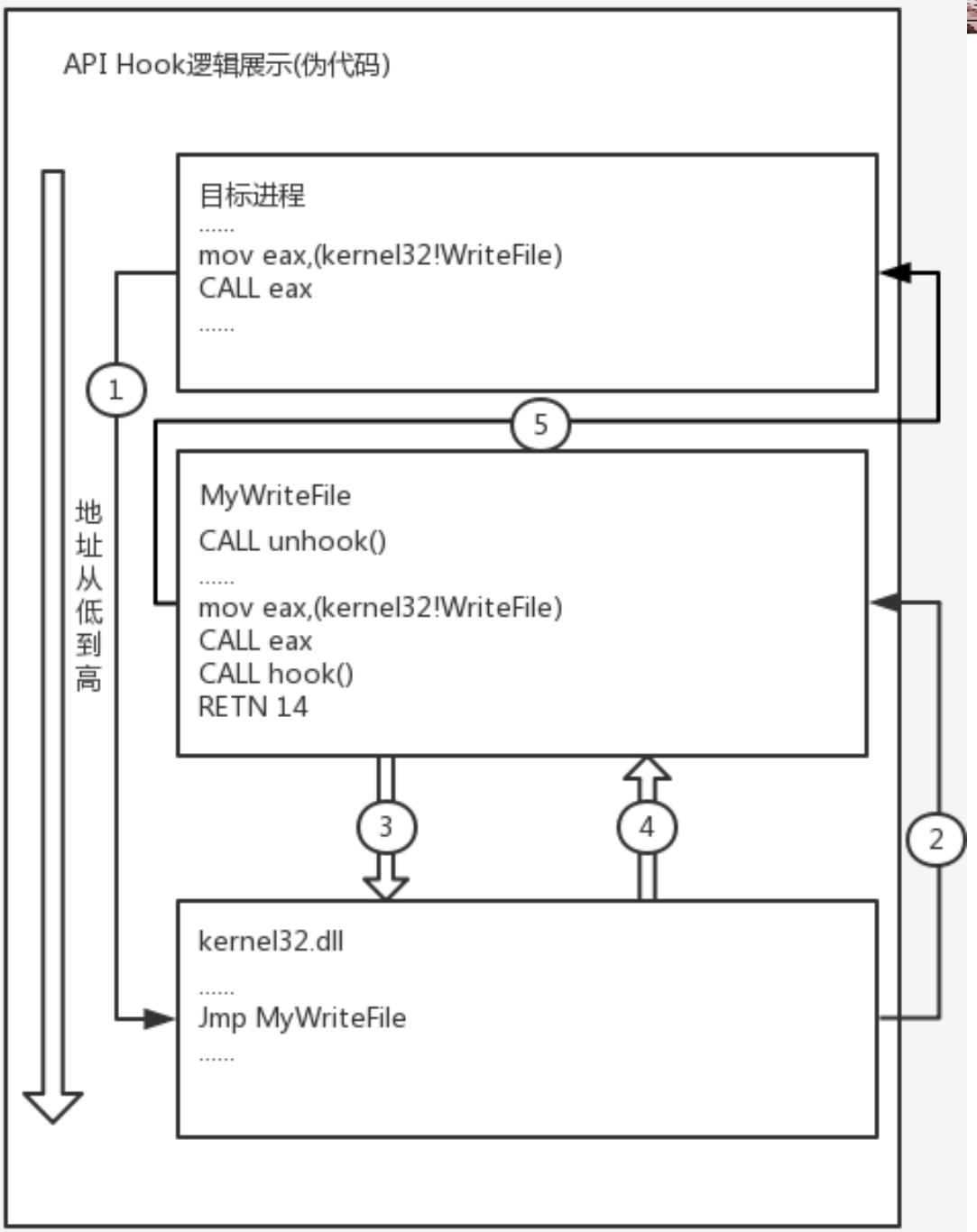
二. API Hook

❒自定义函数MyWriteFile

```
BOOL MyWriteFile(HANDLE hFile, LPCVOID lpBuffer, DWORD nNumberOfBytesToWrite,
LPDWORD lpNumberOfBytesWritten, LPOVERLAPPED lpOverlapped)
{
        FARPROC pFunc;
        unhook();
        pFunc=GetProcAddress(GetModuleHandleA("kernel32.dll"), "WriteFile");
        ((PFWriteFile)pFunc)(hFile, lpBuffer, nNumberOfBytesToWrite, lpNumberOfBytesWritten,
lpOverlapped);
        /*
        执行我们自己的代码
        */
        hook(); //代码逻辑与第二个步骤中main函数的代码相似
        return TRUE;
}
```


二.

❒API Hook逻辑梳理图



二. API Hook

1. 程序从目标进程位置出发，首先是调用了WriteFile函数，然后跳转到了kernel32.dll。
2. 由于此时WriteFile已经被hook，开头的5个字节对应的汇编代码已经变成了JmpMyWriteFile，程序从kernel32.dll跳转到了MyWriteFile当中。
3. 在MyWriteFile中，脱钩了WriteFile函数，执行了我们自己的代码以及WriteFile函数，程序从MyWriteFile位置又再次跳转到了kernel32.dll。
4. 在kernel32.dll中执行完WriteFile函数以后，返回到了MyWriteFile函数当中。
5. 最后再次hook了WriteFile函数，返回到我们自己一开始目标进程的位置。

二. API Hook

- 2 动态调试API Hook
  - 通过IDA来动态调试一下API Hook，用调试器来感受一下API Hook
  - 首先看一下整体的C代码，对程序逻辑有一个初步的印象
  - 程序替换了原本要写入hook文件的“WriteFile”字符串，修改为了“The magic of API Hook”

```
#include<stdio.h>
#include<windows.h>
#include<string.h>
BYTE pOrgByte[5] = { 0, };
typedefBOOL(WINAPI *PFWriteFile)(HANDLE hFile, LPCVOID lpBuffer, DWORD nNumberOfBytesToWrite,
LPDWORD lpNumberOfBytesWritten, LPOVERLAPPED lpOverlapped);
voidunhook()
{
        DWORD dwOldProtect;
        PBYTE pWriteFile;
        FARPROC pFunc;
        pFunc=GetProcAddress(GetModuleHandleA("kernel32.dll"), "WriteFile");
        pWriteFile= (PBYTE)pFunc;
        VirtualProtect(pWriteFile, 5, PAGE_EXECUTE_READWRITE, &dwOldProtect);
        memcpy(pWriteFile, pOrgByte, 5);
        VirtualProtect(pWriteFile, 5, dwOldProtect, &dwOldProtect);
}
BOOL __stdcallMyWriteFile(HANDLE hFile, LPCVOID lpBuffer, DWORD nNumberOfBytesToWrite, LPDWORD
lpNumberOfBytesWritten, LPOVERLAPPED lpOverlapped)
{
        FARPROC pFunc;
        charbuf[] = { "The magic of API Hook!" };
        unhook();
        pFunc=GetProcAddress(GetModuleHandleA("kernel32.dll"), "WriteFile");

        ((PFWriteFile)pFunc)(hFile, buf, strlen(buf), lpNumberOfBytesWritten, lpOverlapped);
        return TRUE;
}
```

```
Int main()
{
        HANDLE hFile;
        HMODULE hKernel32;
        FARPROC pWriteFile;
        PBYTE pEditFunc;
        byte pJmpCode[6] = { 0xE9,0, };
        DWORD dwOldProtect, pOffset,dwWritenSize;
        charbuf[] ="WriteFile";
        hKernel32 =GetModuleHandle(L"kernel32.dll");
        pWriteFile=GetProcAddress(hKernel32, "WriteFile");
        pEditFunc= (PBYTE)pWriteFile;
        if (VirtualProtect(pEditFunc, 5, PAGE_EXECUTE_READWRITE, &dwOldProtect))
        {
                memcpy(pOrgByte, pEditFunc, 5);
                pOffset= (ULONGLONG)MyWriteFile- (ULONGLONG)pWriteFile-5;
                memcpy(&pJmpCode[1], &pOffset, 4);
                memcpy(pWriteFile, &pJmpCode[0], 5);
                VirtualProtect(pWriteFile, 5, dwOldProtect, &dwOldProtect);
        }
        hFile=CreateFile(L"hook", GENERIC_WRITE | GENERIC_READ, NULL, NULL,
CREATE_ALWAYS, 0x80, NULL);
        WriteFile(hFile, buf, strlen(buf), &dwWritenSize, NULL);
        return0;
}
```

二. API Hook

- 配套的程序使用的是**vc6.0**编译的**release**版本，用**ida6.8**打开生成的二进制程序，对程序进行分析

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  HMODULE v3; // eax@1
  FARPROC v4; // esi@1
  HANDLE v5; // eax@3
  DWORD flOldProtect; // [sp+8h] [bp-1Ch]@1
  DWORD NumberOfBytesWritten; // [sp+Ch] [bp-18h]@3
  int v9; // [sp+10h] [bp-14h]@1
  int Buffer; // [sp+18h] [bp-Ch]@1
  int v11; // [sp+1Ch] [bp-8h]@1
  __int16 v12; // [sp+20h] [bp-4h]@1

  LOWORD(v9) = 233;
  *(int *)((char *)&v9 + 2) = 0;
  Buffer = *(_DWORD *)ProcName;
  v11 = dword_405044;
  v12 = word_405048;
  v3 = GetModuleHandleA(ModuleName);
  v4 = GetProcAddress(v3, ProcName);
  if ( VirtualProtect(v4, 5u, 0x40u, &flOldProtect) )
  {
    dword_4052C0 = *(_DWORD *)v4;
    byte_4052C4 = *((_BYTE *)v4 + 4);
    *(int *)((char *)&v9 + 1) = (char *)sub_401060 - (char *)v4 - 5;
    *(_DWORD *)v4 = v9;
    *((_BYTE *)v4 + 4) = (unsigned int)((char *)sub_401060 - (char *)v4 - 5) >> 24;
    VirtualProtect(v4, 5u, flOldProtect, &flOldProtect);
  }
  v5 = CreateFileA(FileName, 0xC0000000, 0, 0, 2u, 0x80u, 0);
  WriteFile(v5, &Buffer, strlen((const char *)&Buffer), &NumberOfBytesWritten, 0);
  return 0;
}
```

二. API Hook

- main函数中代码的主要功能即实现hook，先获得WriteFile的函数地址，对其进行修改，创建一个名为hook的文件，然后写入Buffer里面的内容，Buffer里面的原本内容是WriteFile

```
.data:00405030 ; CHAR ModuleName[]
.data:00405030 ModuleName      db 'kernel32.dll',0      ; DATA XREF: sub_401000+8↑o
.data:00405030                                          ; sub_401060+22↑o ...
.data:0040503D                 align 10h
.data:00405040 ; CHAR aWritefile[]
.data:00405040 aWritefile      db 'WriteFile',0         ; DATA XREF: sub_401000+3↑o
.data:00405040                                          ; sub_401060+1D↑o ...
.data:0040504A                 db    0
.data:0040504B                 db    0
.data:0040504C aTheMagicOfApiH db 'The magic of API Hook!',0 ; DATA XREF: sub_401060+A↑o
.data:00405063                 db    0
.data:00405064 ; CHAR FileName[]
.data:00405064 FileName        db 'hook',0              ; DATA XREF: _main+B5↑o
```


二. API Hook

- 动态调试hook的过程
  - ida菜单栏中选择Local Win32 debugger，通过F2设置断点，在0x40115F，0x4011AE，0x401060地址处下断。然后ida菜单栏中选择Local Win32 debugger，点击左侧的开始按钮，进行调试。
  - 程序成功在0x40115F处断下，这个位置就是即将要修改WriteFile函数地址开头5个字节的地方，edx中保存的就是kernel32.dll中WriteFile的起始地址
  - 此时可看看还没有修改时，入口地址处代码，右键寄存器窗口中的edx寄存器，选择Jump，反汇编窗口就自动跳到了WriteFile的入口地址

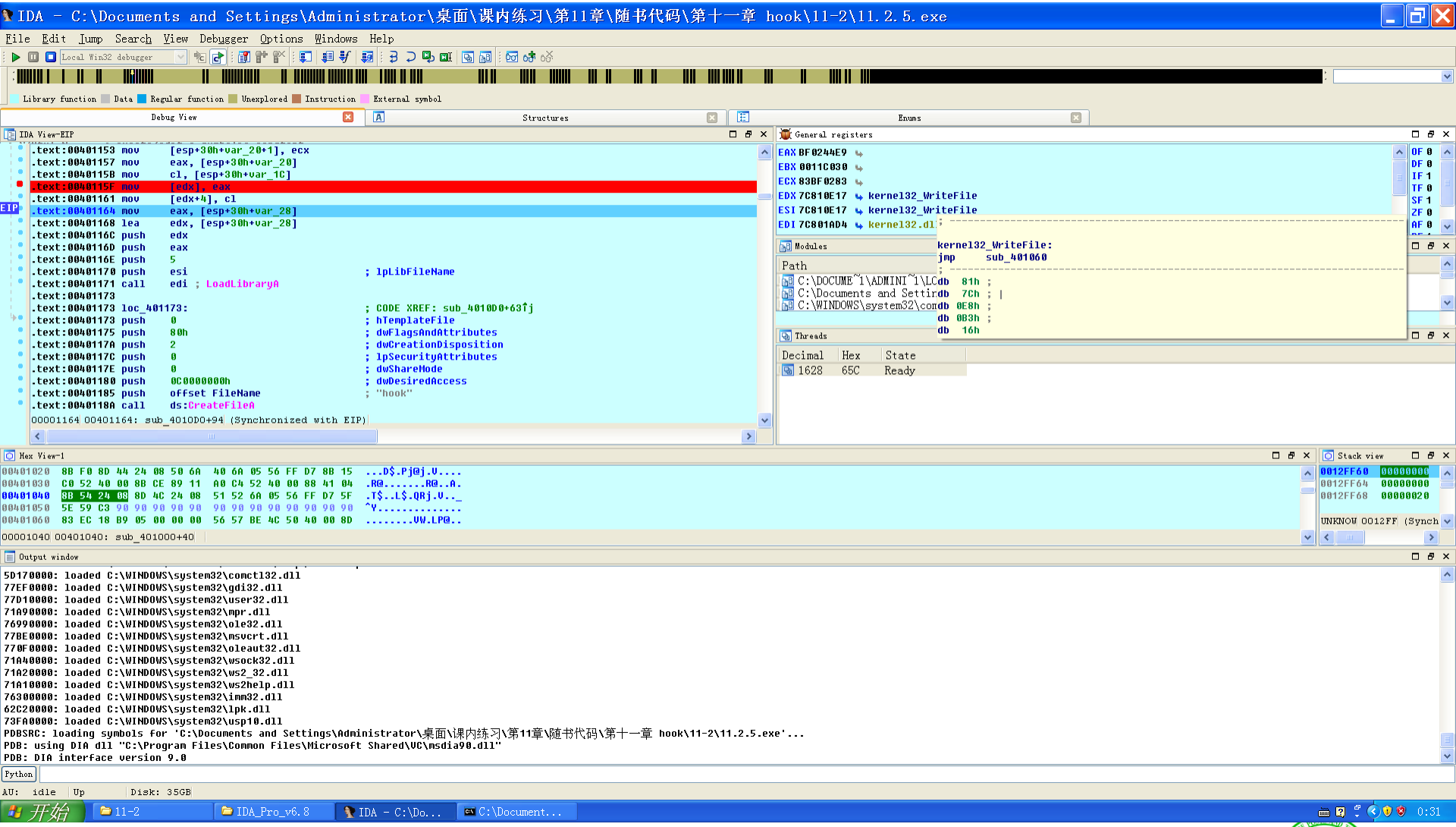
二. API Hook

```
kernel32.dll:7462FC30
kernel32.dll:7462FC30                   ; Attributes: thunk
kernel32.dll:7462FC30
kernel32.dll:7462FC30                   kernel32_WriteFile proc near
kernel32.dll:7462FC30 FF 25 78 0F 64 74 jmp     off_74640F78
kernel32.dll:7462FC30                   kernel32_WriteFile endp
kernel32.dll:7462FC30
```

- F8单步执行两次，再次观察同一个位置，此时WriteFile入口地址变成了下图

```
kernel32.dll:7462FC30                   ; ---------------------------------------
kernel32.dll:7462FC30
kernel32.dll:7462FC30                   kernel32_WriteFile:
kernel32.dll:7462FC30 E9 2B 14 DD 8B    jmp     sub_401060
kernel32.dll:7462FC30                   ; ---------------------------------------
```

- 可以看到，修改之后跳转的位置不再位于kernel32.dll当中，而是我们的MyWriteFile函数，地址0x401060的位置。


IDA - C:\Documents and Settings\Administrator\桌面\课内练习\第11章\随书代码\第十一章 hook\11-2\11.2.5.exe
File Edit Jump Search View Debugger Options Windows Help
Library function Data Regular function Unexplored Instruction External symbol
Debug View
Structures
Enums
IDA View-EIP
.text:00401153 mov [esp+30h+var_20+1], ecx
.text:00401157 mov eax, [esp+30h+var_20]
.text:0040115B mov cl, [esp+30h+var_1C]
.text:0040115F mov [edx], eax
.text:00401161 mov [edx+4], cl
.text:00401164 mov eax, [esp+30h+var_28]
.text:00401168 lea edx, [esp+30h+var_28]
.text:0040116C push edx
.text:0040116D push eax
.text:0040116E push 5
.text:00401170 push esi ; lpLibFileName
.text:00401171 call edi ; LoadLibraryA
.text:00401173 loc_401173: ; CODE XREF: sub_4010D0+63↑j
.text:00401173 push 0 ; hTemplateFile
.text:00401175 push 80h ; dwFlagsAndAttributes
.text:0040117A push 2 ; dwCreationDisposition
.text:0040117C push 0 ; lpSecurityAttributes
.text:0040117E push 0 ; dwShareMode
.text:00401180 push 0C0000000h ; dwDesiredAccess
.text:00401185 push offset FileName ; "hook"
.text:0040118A call ds:CreateFileA
00001164 00401164: sub_4010D0+94 (Synchronized with EIP)
General registers
EAX BF0244E9
EBX 0011C030
ECX 83BF0283
EDX 7C810E17 kernel32_WriteFile
ESI 7C810E17 kernel32_WriteFile
EDI 7C801AD4 kernel32.dl
kernel32_WriteFile:
jmp sub_401060
Modules
Path
C:\DOCUME~1\ADMINI~1\LC
C:\Documents and Settir
C:\WINDOWS\system32\con
Threads
Decimal Hex State
1628 65C Ready
Hex View-1
00401020 8B F0 8D 44 24 08 50 6A 40 6A 05 56 FF D7 8B 15 ...D$.Pj@j.V....
00401030 C0 52 40 00 8B CE 89 11 A0 C4 52 40 00 88 41 04 .R@.....R@..A.
00401040 8B 54 24 08 8D 4C 24 08 51 52 6A 05 56 FF D7 5F .T$..L$.QRj.V.._
00401050 5E 59 C3 90 90 90 90 90 90 90 90 90 90 90 90 90 ^Y..............
00401060 83 EC 18 B9 05 00 00 00 56 57 BE 4C 50 40 00 8D ....VW.LP@..
00001040 00401040: sub_401000+40
Stack view
0012FF60 00000000
0012FF64 00000000
0012FF68 00000020
UNKNOW 0012FF (Synch
Output window
5D170000: loaded C:\WINDOWS\system32\comctl32.dll
77EF0000: loaded C:\WINDOWS\system32\gdi32.dll
77D10000: loaded C:\WINDOWS\system32\user32.dll
71A90000: loaded C:\WINDOWS\system32\mpr.dll
76990000: loaded C:\WINDOWS\system32\ole32.dll
77BE0000: loaded C:\WINDOWS\system32\msvcrt.dll
770F0000: loaded C:\WINDOWS\system32\oleaut32.dll
71A40000: loaded C:\WINDOWS\system32\wsock32.dll
71A20000: loaded C:\WINDOWS\system32\ws2_32.dll
71A10000: loaded C:\WINDOWS\system32\ws2help.dll
76300000: loaded C:\WINDOWS\system32\imm32.dll
62C20000: loaded C:\WINDOWS\system32\lpk.dll
73FA0000: loaded C:\WINDOWS\system32\usp10.dll
PDBSRC: loading symbols for 'C:\Documents and Settings\Administrator\桌面\课内练习\第11章\随书代码\第十一章 hook\11-2\11.2.5.exe'...
PDB: using DIA dll "C:\Program Files\Common Files\Microsoft Shared\VC\msdia90.dll"
PDB: DIA interface version 9.0
Python
AU: idle Up Disk: 35GB
开始
11-2
IDA_Pro_v6.8
IDA - C:\Do...
C:\Document...
0:31

北邮网安学院　崔宝江

二. API Hook

- 摁下F9，到达下一处断点位置，也就是调用WriteFile之前

```
.text:00401185 68 64 50 40 00    push    offset FileName                 ; "hook"
.text:0040118A FF 15 10 40 40 00 call    ds:CreateFileA
.text:00401190 8D 4C 24 0C       lea     ecx, [esp+24h+NumberOfBytesWritten]
.text:00401194 6A 00             push    0                               ; lpOverlapped
.text:00401196 8B D0             mov     edx, eax
.text:00401198 51                push    ecx                             ; lpNumberOfBytesWritte
.text:00401199 8D 7C 24 20       lea     edi, [esp+2Ch+Buffer]
.text:0040119D 83 C9 FF          or      ecx, 0FFFFFFFFh
.text:004011A0 33 C0             xor     eax, eax
.text:004011A2 F2 AE             repne scasb
.text:004011A4 F7 D1             not     ecx
.text:004011A6 49                dec     ecx
.text:004011A7 8D 44 24 20       lea     eax, [esp+2Ch+Buffer]
.text:004011AB 51                push    ecx                             ; nNumberOfBytesToWrite
.text:004011AC 50                push    eax                             ; lpBuffer
.text:004011AD 52                push    edx                             ; hFile
.text:004011AE FF 15 0C 40 40 00 call    ds:WriteFile
.text:004011B4 5F                pop     edi
.text:004011B5 33 C0             xor     eax, eax
.text:004011B7 5E                pop     esi
.text:004011B8 83 C4 1C          add     esp, 1Ch
.text:004011BB C3                retn
.text:004011BB                   _main endp
```

二. API Hook

- F7单步步入WriteFile函数，这时程序会跳到下图的位置，而后到达设置的第三个断点0x401060的位置。
- 进入之后我们反编译一下代码，可以看到这就是C源码中的MyWriteFile函数，而v6则是我们再次调用的WriteFile函数，0x401000处代码对WriteFile函数进行脱钩操作

```
signed int __stdcall sub_401060(int a1, int a2, int a3, int a4, int a5)
{
  HMODULE v5; // eax@1
  FARPROC v6; // edx@1
  char v8; // [sp+8h] [bp-18h]@1

  qmemcpy(&v8, aTheMagicOfApiH, 0x17u);
  sub_401000();
  v5 = GetModuleHandleA(ModuleName);
  v6 = GetProcAddress(v5, aWritefile);
  ((void (__stdcall *)(int, char *, unsigned int, int, int))v6)(a1, &v8, strlen(&v8), a4, a5);
  return 1;
}
```

MyWriteFile函数

二. API Hook

- 以上就是**hook**代码的所有重点，我们直接**f9**结束程序，看看生成的**hook**文件里的内容是什么

```
1  The magic of API Hook!
```


第十一章 Hook入门

- 一. Hook概述
- 二. API Hook
- 三.逆向分析

北邮网安学院　崔宝江

三.逆向分析

- 为巩固hook内容，关于hook的逆向分析题目
- 注意事项：
  - 题目需要解出正确的密码，需要读者输入的用户名是：Welcome_Warrior
  - 对应的题目，一个需要在win10系统中运行，另外一个是需要在win7系统中运行，题目都是相同的，只是运行环境有所不同，在做题的时候需要注意。

三.逆向分析

- 课后练习11-3的程序目录下有练习程序
- 相应的源码放在了11-3源码目录中
- 主要思路为
  - 父进程获取用户输入，然后创建子进程，由子进程获取输入以后，校验输入是否正确，校验逻辑通过hook WriteFile的方式隐藏在了我们自己定义的MyWriteFile函数当中。

三.逆向分析

- 知识点1
  - 从InMemoryOrderModuleList上获取到kernel32.dll的基地址，而不是通过GetModuleHandle这个Windows API。

```
DWORD findPEB()
{
	DWORD pebValue;
	__asm
	{
		mov eax,fs:[0x30]
		mov pebValue,eax
	}
	return pebValue;
}
DWORD calValue1(WORD *a1)
{
	DWORD v1,v3;
	v3 =0;
	while(*a1)
	{
		v1 = (WORD)*a1;
		++a1;
		v3 = v1 + ((v3 <<19) | ((unsigned__int64)v3 >>13));
	}
	return v3;
}
DWORD findKernel32()
{
	DWORD pebValue=findPEB();

	DWORD v1 =*(DWORD *)(pebValue+12);
	DWORD *v3 =*(DWORD **)(v1 +20);
	DWORD *v4 =*(DWORD **)(v1 +20);
	do
	{
		if(calValue1((WORD *)v3[10]) == kernel32Value)
		{
			return v3[4];
		}
		v3 = (DWORD *)*v3;
	} while (v3 && v3 != v4);
```

三.逆向分析

- **首先findPEB()函数获取的进程环境块PEB的地址，通过PEB，在偏移为12的地方找到名为Ldr的结构体，通过Ldr偏移20的地方就是InMemoryOrderModuleList了**
  - 1、通过fs:[30h]获取当前进程的_PEB结构
  - 2、通过_PEB的Ldr成员获取_PEB_LDR_DATA结构
  - 3、通过_PEB_LDR_DATA的InMemoryOrderModuleList成员获取结构信息。

三.逆向分析

- InMemoryOrderModuleList结构是一个链表，当前节点偏移40的位置是对应的动态链接库字符串，比如说kernel32.dll，而偏移16的位置则是该DLL的基地址，偏移为0的位置是该链表的下一个节点。
- 通过calValue1函数对字符串进行计算，如果取得的值与kernel32Value相等，即是kernel32.dll，那么就返回它的基地址。

三.逆向分析

- 注
  - **FS寄存器指向当前活动线程的TIB（Thread Information Struct)结构，其中偏移0x30的位置指向了PEB**

三.逆向分析

```
typedef struct _PEB
 {
 UCHAR InheritedAddressSpace;
 UCHAR ReadImageFileExecOptions;
 UCHAR BeingDebugged;
 UCHAR SpareBool;
 PVOID Mutant;
 PVOID ImageBaseAddress;
 PPEB_LDR_DATA Ldr;
 }PEB,*PPEB;
```


三.逆向分析

- typedef struct _PEB_LDR_DATA
  {
  DWORD Length;
  UCHAR Initialized;
  PVOID SsHandle;
  LIST_ENTRY InLoadOrderModuleList;
  LIST_ENTRY InMemoryOrderModuleList; //按内存顺序
  LIST_ENTRY InInitializationOrderModuleList;
  PVOID EntryInProgress;
  }PEB_LDR_DATA,*PPEB_LDR_DATA;

三.逆向分析

- 知识点2
  - 从kernel32.dll的导出表中找到相应函数的地址，并赋值于变量中，而不是直接调用函数API。

```
DWORD calValue2(BYTE *a1)
{
        DWORD v1,v3;
        v3 =0;
        while(*a1)
        {
                v1 =*a1++;
                v3 = v1 + ((v3 <<19) | ((unsigned__int64)v3 >>13));
        }
        return v3;
}
DWORD findGetProcAddress(DWORD kernel32Addr,DWORD funcValue)
{
        DWORD
exportTable,addressOfFunctions,addressOfNames,addressOfNameOrdinals,numberOfNames;
        exportTable= (*(DWORD *)(*(DWORD *)(kernel32Addr +60) + kernel32Addr +120) + kernel32Addr);
        addressOfFunctions=*(DWORD *)(exportTable+0x1c) + kernel32Addr;
        addressOfNames=*(DWORD *)(exportTable+0x20) + kernel32Addr;
        addressOfNameOrdinals=*(DWORD *)(exportTable+0x24) + kernel32Addr;
        numberOfNames=*(DWORD *)(exportTable+0x18);
        for(inti=0;i<numberOfNames;i++)
        {
                if(calValue2((BYTE *)(*(DWORD *)(addressOfNames+4*i) + kernel32Addr)) ==funcValue)
                        return*(DWORD *)(addressOfFunctions+4**(WORD
*)(addressOfNameOrdinals+2*i)) + kernel32Addr;
        }
        return 0;
}
```

三.逆向分析

- findGetProcAddress函数的作用
  - 通过知识点1中获得的kernel32的值，带入findGetProcAddress函数，通过比较funcValue的值找到对应的函数API地址。
  - 这里比较的funcValue的值同样是通过calValue2函数得到，算法和知识点1中相同，只不过知识点1中计算的字符串是unicode字符，而知识点2中的字符串是utf-8字符。
    - 比如将CreateFile这个字符串进行calValue2的计算，将得到的返回值与对应的funcValue作比较，如果相同，则说明此时找到的API地址是CreateFile函数的地址。

三.逆向分析

- 知识点3
  - 从导出表中获取相应函数地址的时候，没有通过比较字符串名称的方式来获取函数地址，而是对字符串名称进行了算法的计算，通过比较那一串值来确定是否是对应的API函数。
  - 这两个函数即是对应计算字符串值的算法函数，知识点1和知识点2中皆有讲解

三.逆向分析

```
DWORD calValue1(WORD *a1)
{
        DWORD v1,v3;
        v3 =0;
        while(*a1)
        {
                v1 = (WORD)*a1;
                ++a1;
                v3 = v1 + ((v3 <<19) | ((unsigned__int64)v3 >>13));
        }
        return v3;
}
DWORD calValue2(BYTE *a1)
{
        DWORD v1,v3;
        v3 =0;
        while(*a1)
        {
                v1 =*a1++;
                v3 = v1 + ((v3 <<19) | ((unsigned__int64)v3 >>13));
        }
        return v3;
}
```


三.逆向分析

- 知识点4
  - 程序中使用了父进程创建了子进程，由子进程来完成正确用户名和正确密码的校验，增加了调试的难度。
  - 上述代码中，首先是创建了互斥量，作用是当父进程创建子进程以后，子进程再行创建互斥量之时，则会返回**ERROR_ALREADY_EXISTS**，然后由子函数来完成对用户名和密码的校验逻辑。

```
BOOL createChildProcess(BYTE Username[], BYTE Password[])
{
        BOOL result;
        TCHAR UP[100] = { 0, };
        BYTE UnamePword[100] = { 0. };
        TCHAR fileName[MAX_PATH];
        /*处理用户名和密码的代码省略*/
((myGetModuleFileName)pGetModuleFileNameW)(NULL, (LPWSTR)fileName, 100);
        size_tconvertedChars=0;
        mbstowcs_s(&convertedChars, (LPWSTR)UP, strlen((PSTR)UnamePword) +1, (PSTR)UnamePword, _TRUNCATE);
        STARTUPINFOW si={ sizeof(si) };
        PROCESS_INFORMATION pi;
        result = ((myCreateProcess)pCreateProcessW)((LPWSTR)fileName, (LPWSTR)UP, 0, 0, 0, 0, 0, 0, &si, &pi);
        }
        return result;
}
intmain(intargc,TCHAR*argv[])
{
/*main函数中其他的初始化功能省略*/
HANDLE hCreateMutex;
hCreateMutex= ((myCreateMutex)pCreateMutexW)(NULL, FALSE, L"Get Flag?");
if (GetLastError() == ERROR_ALREADY_EXISTS)
{
        /*子进程进行逻辑校验省略*/
}
else
{
/*输入用户名和密码的代码省略*/
createChildProcess(Username, Password);
system("pause");
}
return 0;
}
```


三.逆向分析

- 知识点5
  - 使用API Hook的方式hook了WriteFile函数，使得真正的校验逻辑隐藏在了hook的函数中。
  - 对于hook WriteFile函数，在逆向代码时看到上述代码应该是不会陌生

三.逆向分析

```
voidhook_begin()
{
        DWORD dwOldProtect,pOffset;
        BYTE pJmpCode[6] = { 0xE9,0, };
        HMODULE hModule;
        PBYTE pWriteFile;
        FARPROC pFuncOrg;
        hModule= ((myGetModuleHandle)pGetModuleHandleA)("kernel32.dll");
        pFuncOrg=(FARPROC)(((myGetProcAddress)pGetProcAddress)(hModule, "WriteFile"));
        pWriteFile= (PBYTE)pFuncOrg;
        if (((myVirtualProtect)pVirtualProtect)(pWriteFile, 5, PAGE_EXECUTE_READWRITE,
&dwOldProtect))
        {
                memcpy(pOrgByte, pWriteFile, 5);
                pOffset= (ULONGLONG)MyWriteFile- (ULONGLONG)pWriteFile-5;
                memcpy(&pJmpCode[1], &pOffset, 4);
                memcpy(pWriteFile, &pJmpCode[0], 5);
                ((myVirtualProtect)pVirtualProtect)(pWriteFile, 5, dwOldProtect,
&dwOldProtect);
        }
}
```

三.逆向分析

- 知识点6
  - 为增强迷惑性，判断成功条件的位置，增加了一个陷阱函数，增加逆向的分析难度，在陷阱函数里面，使用了简单的花指令，只需要手动将其清除，就能恢复反编译。

三.逆向分析

```
 hFile= ((myCreateFile)pCreateFileW)(L"PowerfulDatabase", GENERIC_WRITE |
GENERIC_READ, NULL, NULL, CREATE_ALWAYS, 0x80, NULL);
 hook_begin();
 ((myWriteFile)pWriteFile)(hFile, UnamePword, strlen((char*)UnamePword),
&dwWritenSize, 0);
 if (fake_flag(UnamePword))
        {
                wprintf(L"Good! The flag is the Dubhe{Password}!\n");
        }
        else
        {
                wprintf(L"Wrong!!!\n");
        }
```


三.逆向分析

- 上述代码中的**hook_begin**即是**hook**了**WriteFile**函数，**fake_flag**即是验证**flag**的假逻辑，在其中添加了简单的几处花指令，熟悉前面章节的花指令内容的读者，应该能够快速地手动排除花指令，令其正常反编译。

三.逆向分析

- 解题思路
  - 关键点即是找到hook WriteFile的点，hook函数位置如图

```
int sub_4012D0()
{
  int v0; // eax@1
  int v1; // eax@1
  int v2; // esi@1
  int result; // eax@1
  _BYTE v4[5]; // [sp+4h] [bp-Ch]@1
  int v5; // [sp+Ch] [bp-4h]@1

  v4[0] = -23;
  v0 = dword_40441C("kernel32.dll");
  v1 = dword_404410(v0, "WriteFile");
  v2 = v1;
  result = dword_404438(v1, 5, 64, &v5);
  if ( result )
  {
    dword_404430 = *(_DWORD *)v2;
    byte_404434 = *(_BYTE *)(v2 + 4);
    *(_DWORD *)&v4[1] = (char *)sub_401240 + -v2 - 5;
    *(_DWORD *)v2 = *(_DWORD *)v4;
    *(_BYTE *)(v2 + 4) = v4[4];
    result = dword_404438(v2, 5, v5, &v5);
  }
  return result;
}
```

三.逆向分析

- 如果走进了陷井函数，不管去不去除花指令，都可以看到**username**和**password**是随机产生的，**srand(time(NULL))**，所以这里肯定是误区，反过去继续分析，发现**API hook**，求解**flag**。
- 用题目已知的**username**：**Welcome_Warrior**，分析**hook**函数，求解**flag**。

三.逆向分析

- 求解正确密码代码

```
#!/usr/bin/env python
#-*- coding:utf-8 -*-
username ='Welcome_Warriorabcdefgh'
cmpStr= ['13e0', '6a0', '1b60', '670', '19c0', '570', '16a0', '540', '16c0', '490', '1ca0', '688', '1780', '4f8', '1a20', '510',
'19e0', '620', '1bc0', '4c0', '12e0', '6a8', '19e0']
ans=''
foriinrange(len(cmpStr)):
        if (i&1):
                tmp=int(cmpStr[i],16) >>3
        else:
                tmp=int(cmpStr[i],16) >>5
        ans+=chr(tmp-ord(username[i]))
printans
```

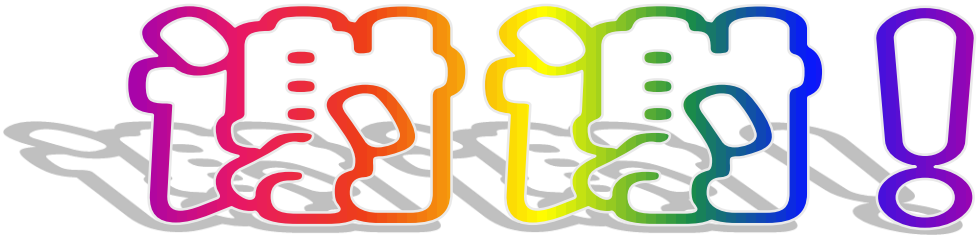

三.逆向分析

- 提交上述题目的writeup

小结

- Windows中的hook方法
  - Message Hook，API Hook，IAT Hook等
- API Hook及其动态调试
- 逆向分析

Q & A



北邮网安学院　崔宝江