19030100036 董津玮

一、 程序 1 （RE_LAB1.cpp）

1. 该程序需要实现创建一个 OllyDbg 进程，核心是使用 CreateProcess()函数创建进程

```
CreateProcessA(ollydbg_path, startArg, NULL, NULL, FALSE, NULL, NULL, NULL,
&si, &pi)
```

2. 由于 OllyDbg 需要管理员权限完成部分功能，所以在创建进程前先要通过进程令牌提升权限

```
int EnableDebugPriv(const char* name)
{
    HANDLE hToken;
    TOKEN_PRIVILEGES tp;
    LUID luid;

    OpenProcessToken(GetCurrentProcess(), TOKEN_ADJUST_PRIVILEGES |
TOKEN_QUERY, &hToken);

    LookupPrivilegeValue(NULL, (LPCWSTR)name, &luid);
    tp.PrivilegeCount = 1;
    tp.Privileges[0].Attributes = SE_PRIVILEGE_ENABLED;
    tp.Privileges[0].Luid = luid;

    int ret = AdjustTokenPrivileges(hToken, 0, &tp,
sizeof(TOKEN_PRIVILEGES), NULL, NULL);
    return ret;
}
```

二、 程序 2 （RE_LAB2.cpp）

1. 该程序需要在新线程中用 MessageBox 显示 kernel32.dll 模块在系统中的路径以及当前线程 ID，涉及的主要函数如下：
   a) MessageBoxA()： 显示一个 MessageBox
   b) GetModuleHandle()： 通过模块名取得当前进程某个模块的句柄
   c) GetModuleFileName()： 通过模块句柄取得该模块在文件系统中的路径
   d) GetProcAddress()： 取得模块中某个函数的起始地址
   e) CreateThread()： 创建线程
   f) WaitForSingleObject()： 等待线程结束

2. 关键语句

a) 创建线程

```
HANDLE msgThreadHandle = CreateThread(NULL, 0, showMsg, dllName, 0, NULL);
```

b) 取得模块路径

```
GetModuleFileNameA(GetModuleHandleA((LPCSTR)targetModuleName), nameBuf,
MAX_PATH);
```

c) 取得 GetCurrentThreadId 函数的起始地址

```
FARPROC GetThreadIdStrAddr= GetProcAddress(GetModuleHandleA("kernel32"),
"GetCurrentThreadId");
```

d) 显示 MessageBox 输出上面结果

```
MessageBoxA(NULL, msgBuf, "Message", MB_YESNO);
```

e) 等待线程结束

```
WaitForSingleObject(msgThreadHandle, INFINITE);
```