远程线程注入

思路

加载DLL

1. 获取`LoadLibrary`的地址（系统库函数在同一台机子上不同进程间的地址一般是一样的）
2. 在目标进程中申请内存，写入**DLL**路径
3. 创建远程线程

卸载DLL

1. 获取模块句柄，由`GetExitCodeThread`获取
2. 获取`FreeLibrary`的地址
3. 创建远程线程

相关函数

- 创建远程线程

```
HANDLE CreateRemoteThread(
  HANDLE                 hProcess,
  LPSECURITY_ATTRIBUTES  lpThreadAttributes,
  SIZE_T                 dwStackSize,
  LPTHREAD_START_ROUTINE lpStartAddress,    // 目标进程中的地址
  LPVOID                 lpParameter,
  DWORD                  dwCreationFlags,
  LPDWORD                lpThreadId
);
```

- 创建虚拟内存空间

```
LPVOID VirtualAllocEx(
  HANDLE hProcess,
  LPVOID lpAddress,     // 为NULL，系统自动分配一个地址
  SIZE_T dwSize,
  DWORD  flAllocationType,
  DWORD  flProtect
);
```