2021/04/02_壳_第5课_补课(函数转发、随机基址重定位)

笔记本: 壳
创建时间: 2021/4/2 星期五 10:47
作者: ileemi

函数转发

dll 中的转发函数通过文件地址计算其在内存中的地址后，访问该地址，地址起始位置开始存储的是转发函数的名称（在dll中实现的导出函数，其代码都在dll中。而转发的函数，其在地址是一个字符串）。

导出函数对应的地址是代码还是字符串可通过 "地址的值" 进行区分。

> 导出函数的地址是字符串时，该地址和数据目录是有一定关系的。判断该地址是否在导出表的范围内，如果在该范围内，就可以判断其是一个转发函数，反之，说明是本dll的导出函数，该函数的实现在本dll内，该地址就可以直接使用。

对于转发函数，可通过对字符串进行解析，确定其真实的导出函数，使用 LoadLibrary 加载dll，然后使用 GetProcAddress 获取导出函数所在模块中的地址。

随机基址 重定位

> 重定位表和导出表的大小必要时可做为参考。