DLL分析注意事项

实验：7-3， 3-2， 5-1， 9-3， 11-2， 11-3，12-1，17-2

静态分析

1. 大部分分析过程和EXE文件是一样的，主要需要注意导出函数
2. 在IDA中打开，在exports子窗口查看其导出函数，双击查看其代码

动态分析

1. 执行方式：
    - 使用`rundll32.exe [DLLname], [Export/ordinal] [arguments]`执行导出函数
    - 可以修改PE header中，位于`IMAGE_FILE_HEADER`中的`IMAGE_FILE_DLL(0x2000)`标志，将DLL变成EXE文件，直接执行其`DLLMain`函数
2. 如果DLL文件的导入或导出函数中存在`ServiceMain`等与服务相关的函数，说明其会安装服务，可以使用导出函数`Install`或者`InstallService`进行安装，若没有合适的安装函数，可以使用`sc`命令，或者手动修改注册表。最后`net start [ServiceName]`启动服务
3. 在使用procmon监控其执行时，`Process Name`应该输入`rundll32.exe`
4. DLL文件启动之后，可以在procexp中使用`Find->Find Handle or DLL`进行搜索，查看哪个进程使用了该DLL
5. 在Ollydbg中，导入DLL文件之后，点击运行，运行停止后，选择`Debug->Call DLL Export`，可以调用某个导出函数，设置其参数，选择`Pause after call`，对其进行调试