

**恶意代码课程实验报告**

**实验五**

****

学 院 网络空间安全学院

专 业 信息安全、法学

学 号 2111454

姓 名 李潇逸

班 级 信息安全、法学

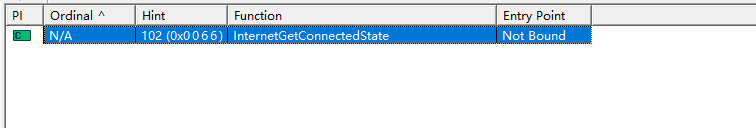
1. **实验环境**

VMWARE，Windows11

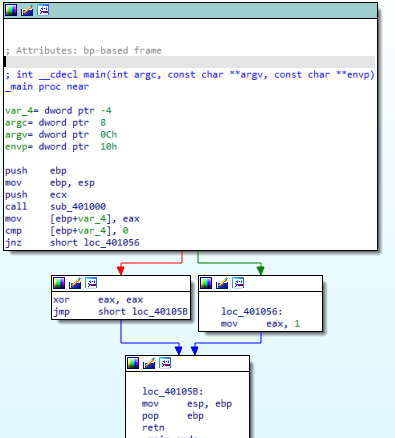
1. **实验工具**

IDA，YARA

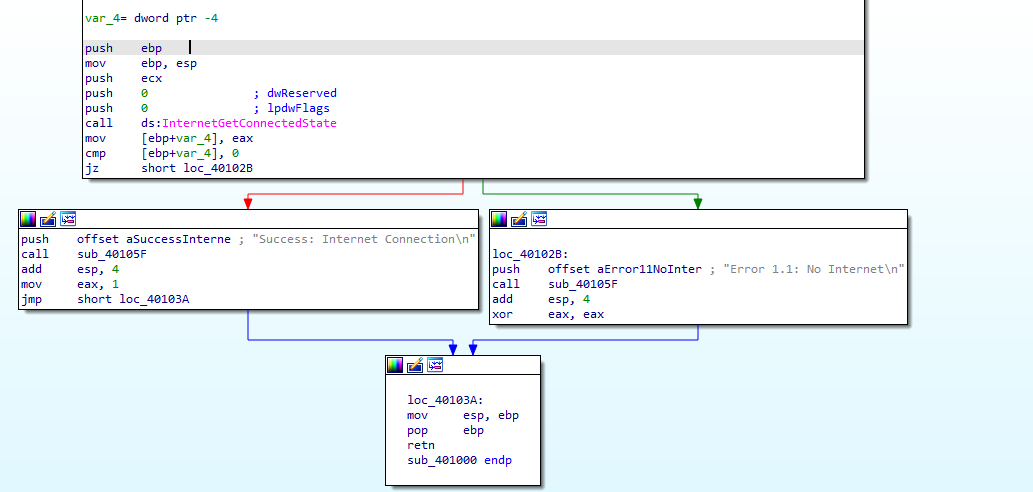
1. **实验过程**
2. **Lab6-1**
3. **静态分析发现了InternetGetConnectedState函数**



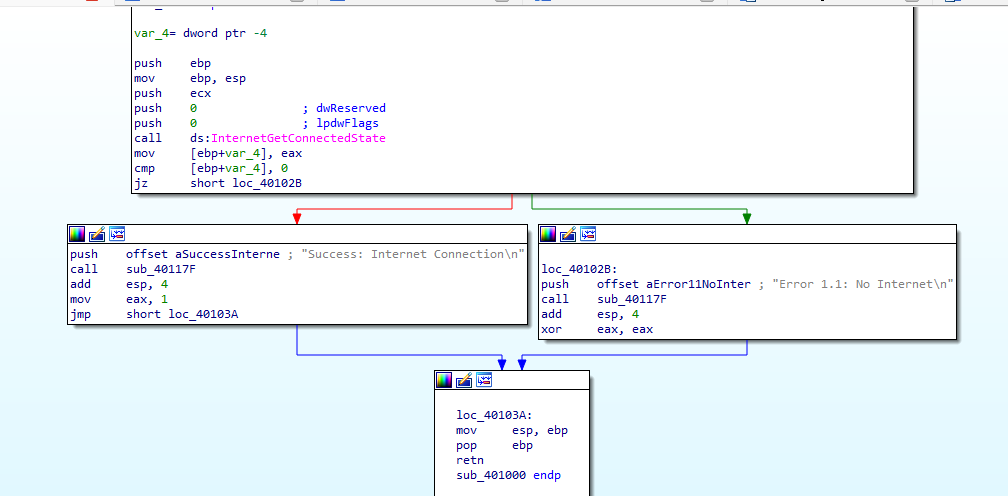
**打开IDA后发现如下内容**



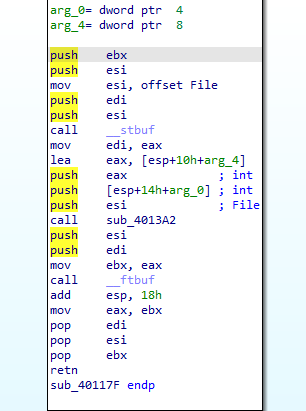
**在main中可以发现调用了401000的函数，该函数是一个if函数**



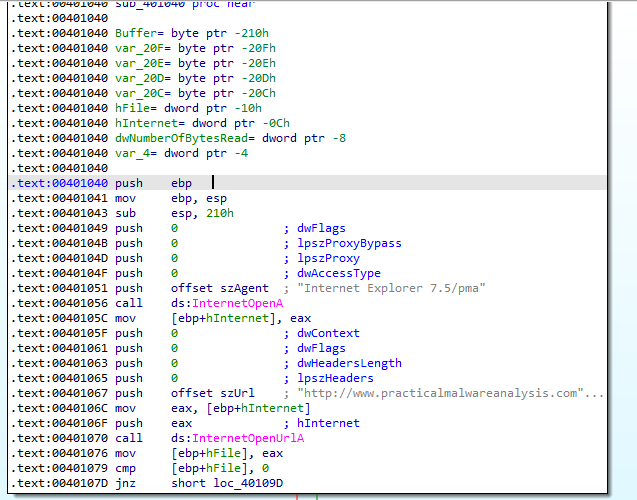
1. **Printf**
2. **该程序检查是否有一个可用的Internet连接。如果找到可用连接，就打印“Success:Internet Connection”，否则，打印“Error 1.1:No Internet”。恶意代码在连接Internet之前，可以使用该程序来检查是否存在一个连接。**
3. **Lab06-02**
4. **是if函数，判断是否有网络链接**



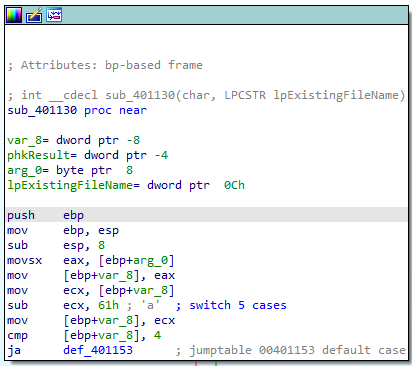
1. **调用了printf**



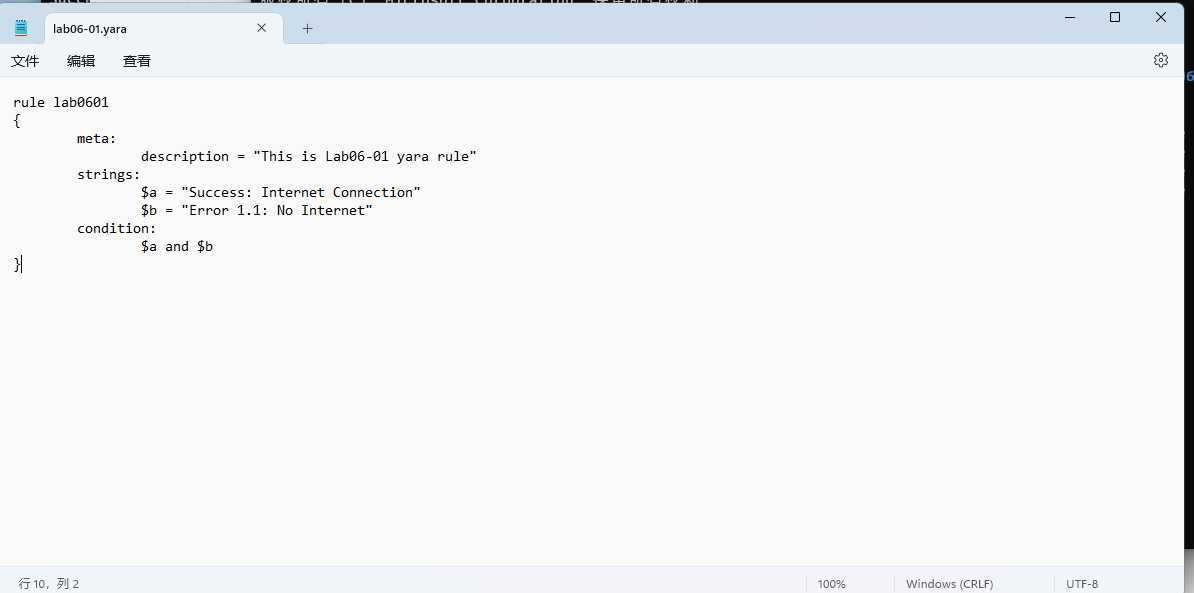
1. **从相关网址中下载内容**



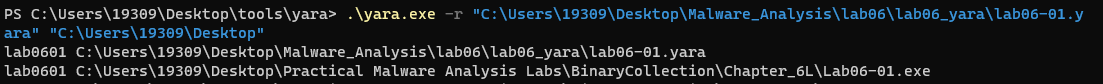
1. **调用InternetReadFile，将读到的字符存入字符数组**
2. **将Internet Explorer 7.5/pma作为User-Agent，从http://www.practicalmalwareanalysis.com下载网页**
3. **程序首先判断是否存在一个可用的Internet连接，如果不存在就终止运行。否则，程序使用一个独特的用户代理尝试下载一个网页。该网页包含了一段由<!--开始的 HTML注释，程序解析其后的那个字符并输出到屏幕,输出格式是“Success:Parsed command isX”,其中X就是从该HTML**
4. **Lab06-03**
5. **新增了0x401271函数为printf和0x401130**
6. **一个为从html的注释得来的指令字符，另一个为函数名本身**



1. **包含一个switch和一个跳转表**
2. **打印错误信息，删除文件，创建文件夹，设置注册表项值，复制文件或休眠**
3. **Software\\Microsoft\\Windows\\CurrentVe和C:\\Temp\\cc.exe可作为标志**
4. **该程序先检查是否存在有效的Internet连接。如果找不到，程序直接终止。否则，该程序会尝试下载一个网页,该网页包含了一段以<!--开头的HTML注释。该注释的第一个字符被用于switch语句来决定程序在本地系统运行的下一步行为，包括是否删除一个文件、创建一个目录、设置一个注册表run键、复制一个文件或者休眠100秒。**
5. **Lab06-04**
6. **检查了网络链接方法**
7. **增加了for循环**
8. **0x401040使用参数**
9. **运行24H**
10. **Internet Explorer 7.50/pma%d %d是指运行时间**
11. **首先，程序会检查是否有可用的Internet连接。如果找不到，程序就终止运行。否则，程序使用一个独特的User-Agent来下载一个网页，这个User-Agent包含了一个计数器，用于说明程序已经运行了多少分钟。下载下来的网页中包含了以<!--开头的HTML注释代码，这段注释代码中接下来的第一个字符被用于一个switch 语句，以决定接下来在本地系统的行为。其中包含了一些硬编码的行为，包括删除一个文件、创建一个目录、设置一个注册表run键、复制一个文件、休眠100秒等。该程序会运行24小时后终止。**
12. **Yara练习**
13. **Lab06-01**



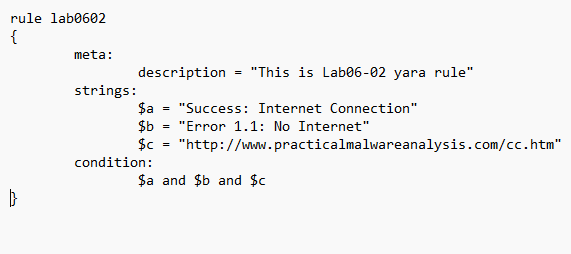
**运行后发现可成功抓取相应的恶意代码**



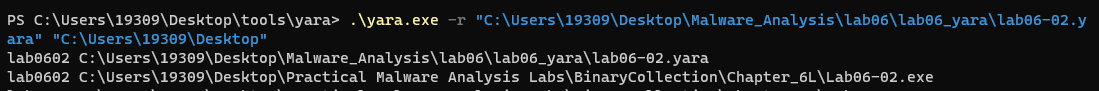
**共执行了7775.5306ms**



1. **Lab06-02**



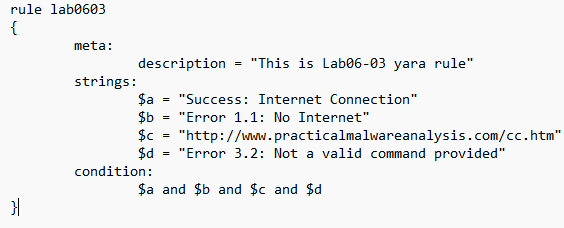
**运行后发现可成功抓取相应的恶意代码**



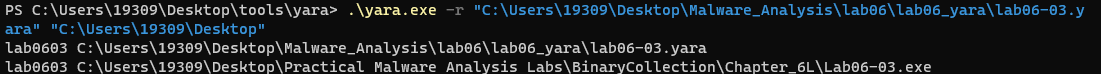
**共执行了2871.5047ms**



1. **Lab06-03**



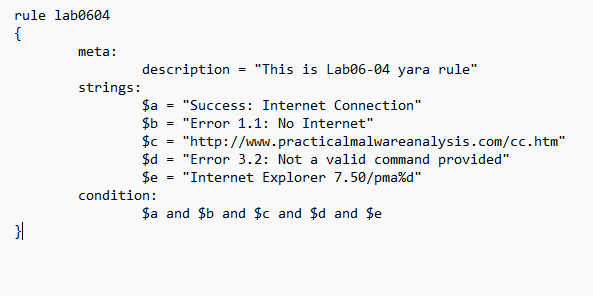
**运行后发现可成功抓取相应的恶意代码**



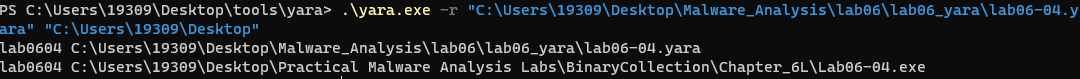
**共执行了6000.3624ms**



1. **Lab06-04**



**运行后发现可成功抓取相应的恶意代码**



**共执行了8614.8786ms**



1. **实验心得**

**初步学习了如何使用工具进行恶意代码分析，对恶意代码和恶意代码分析工具有了更深的理解。**