

**恶意代码课程实验报告**

**实验六：Windows恶意代码**

****

学 院 网络安全学院

专 业 信息安全

学 号 2110688

姓 名 史文天

班 级 1063

1. **实验目的**

**完成课本Lab6的实验内容，编写Yara规则，并尝试IDA Python的自动化分析。**

1. **实验原理**

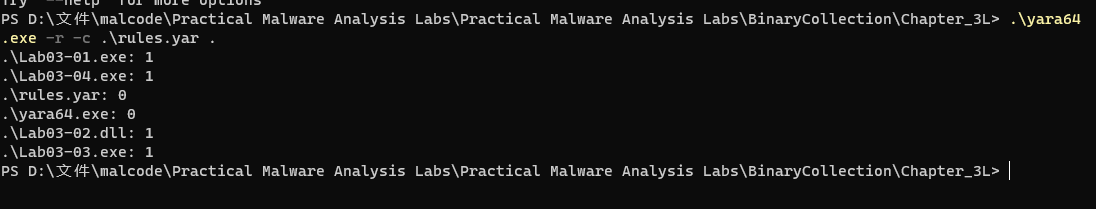
**配置XP虚拟机环境，安装动态、静态分析工具，使用动态分析工具。**

1. **实验过程**
2. **Lab06-01**
3. **由main函数调用的唯一子过程中发现的主要代码结构是什么？**
4. **位于0x40105F的子过程是什么？**
5. **这个程序的目的是什么？**
6. **Lab03-02**
7. **main函数调用的第一个子过程执行了什么操作？位于0x40105F的子过程是什么?**
8. **位于0x40117F的子过程是什么？**
9. **被main函数调用的第二个子过程做了什么？**
10. **在这个子过程中使用了什么类型的代码结构？**
11. **在这程序中有任何基于网络的指示吗？**
12. **这个恶意代码的目的是什么？**
13. **Lab06-03**
14. **比较在main函数与实验6-2 的main函数的调用。从main中调用的新的函数是什么？**
15. **这个新的函数使用的参数是什么？**
16. **这个函数包含的主要代码结构是什么？**
17. **这个函数能够做什么？**
18. **这个恶意代码中有什么本地特征吗？**
19. **这个恶意代码的目的是什么?**
20. **Lab03-04**
21. **在实验6-3 和6-4 的 main 函数中的调用之间的区别是什么？**
22. **什么新的代码结构已经被添加到 main 中？**
23. **这个实验的解析HTML的函数和前面实验中的那些有什么区别？**
24. **这个程序会运行多久？（假设它已经连接到互联网。)**
25. **在这个恶意代码中有什么新的基于网络的迹象吗？**
26. **这个恶意代码的目的是什么？**
27. **Yara规则**

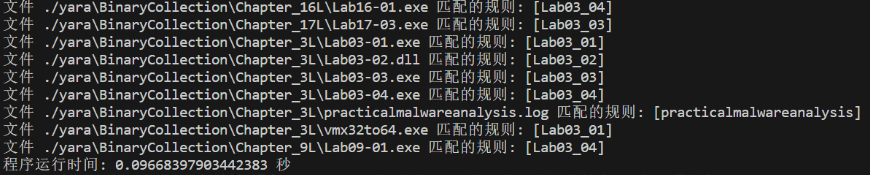
**根据以上分析结果，同时利用Yaragen工具，得到Yara规则如下。**

1. rule Lab03\_01 {

**运行结果如下，可看到成功匹配所有文件。**



**在存放所有样例的文件夹下测试其检测效率，结果如下。**



1. **实验结论及心得体会**
2. **尝试了各种动态分析工具，对动态分析有了一定了解。**
3. **了解了更多恶意代码的形式和特征。**