

**恶意代码课程实验报告**

**实验三：基本动态分析**

****

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**

**完成教材Lab3的实验内容，编写Lab3样本的Yara引擎规则，并测试规则的执行效率。**

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. **Lab03-01**
3. **找出这个恶意代码的导入函数与字符串列表？**

**使用PEiD打开，检测加壳信息。如图所示，可以看到壳为PEncrypt 3.1 Final -> junkcode**

**下面使用Strings查看文件的字符串，可以看到一些诸如WinVMX32、VideoDriver、vmx32to64.exe、注册表位置、注册表键值、url等信息。如下图所示。**

1. **这个恶意代码在主机上的感染迹象特征是什么？**
2. **这个恶意代码是否存在一些有用的网络特征吗？如果存在，它们是什么？**
3. **Lab03-02**
4. **你怎样才能让这个恶意代码自行安装?**
5. **在安装之后，你如何让这个恶意代码运行起来？**
6. **你怎么能找到这个恶意代码是在哪个进程下运行的？**
7. **你可以在procmon工具中设置什么样的过滤器，才能收集这个恶意代码的信息？**
8. **这个恶意代码在主机上的感染迹象特征是什么？**
9. **这个恶意代码是否存在一些有用的网络特征码？**
10. **Lab03-03**
11. **当你使用Process Explorer 工具进行监视时，你注意到了什么？**
12. **你可以找出任何的内存修改行为吗？**
13. **这个恶意代码在主机上的感染迹象特征是什么？**
14. **这个恶意代码的目的是什么？**
15. **Lab03-04**
16. **当你运行这个文件时，会发生什么呢？**
17. **是什么原因造成动态分析无法有效实施？**
18. **是否有其他方式来运行这个程序？**
19. **Yara规则**
20. **实验结论及心得体会**
21. **了解了虚拟机的安装与配置**
22. **了解并安装了多种静态和动态分析使用的工具，为后续实验打下基础。**