

**恶意代码课程实验报告**

**实验二：虚拟机技术**

****

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**

**1. 虚拟机的安装和配置过程；2. 静态分析工具的功能和安装过程；3. 动态分析工具的功能和安装过程。**

1. **实验原理**

**配置XP虚拟机环境，安装动态、静态分析工具。**

1. **实验过程**
2. **配置病毒分析虚拟机**
3. **虚拟机中安装静态分析工具**
4. **虚拟机中安装动态分析工具**
5. **实验结论及心得体会**
6. **对恶意代码调用函数实现攻击的方式有了进一步了解。**
7. **对文件加壳脱壳有了初步了解，学会了如何判断加壳类型，以及如何脱壳。**
8. **初步了解了Yara规则的编写，可以针对文件编写对应的Yara规则。**