# 实验三、恶意代码分析实验

## 一、实验学时

2次课

## 二、实验内容

1、掌握恶意代码分析环境的构建

2、掌握常用恶意代码分析工具的使用

3、完成一个恶意代码样本分析，并撰写分析报告。

## 三、实验阶段

（一）恶意代码分析技能学习



（二）恶意代码样本分析实践

利用掌握的技能，分析一个实际的恶意代码样本，撰写分析报告。在完成第1阶段的学习后，向老师索取恶意代码样本。

## 四、实验工具

1. 虚拟机软件
2. IDA Pro
3. OllyDbg
4. Sysinternals Suite

https://download.sysinternals.com/files/SysinternalsSuite.zip

1. 课程视频中用到的其它软件

## 五、实验报告及提交要求

（一）提交内容

恶意代码分析报告。至少包括内容要求：

1. 样本行为的初步观察

**（提示：选择一个免费的恶意代码线上分析沙箱，在其中观察样本行为。）**

1. 样本行为的详细分析

**（要求：在自己构建的恶意代码分析环境中开展分析。）**

1. 行为1：XXX

**（提示：描述样本观察过程，所得到的观察结论，通过静态分析和动态分析，解释所观察到的样本行为。必须提供关键截图。）**

1. 行为2：XXX

**（提示：同上。）**

**n）……**

1. 样本危害性

**（提示：基于以上分析，分条描述该样本可能给用户计算机系统带来的危害）**

1. 防护建议

**（提示：针对普通计算机用户，提出具有可操作性的防护建议。）**

（二）提交要求

2021年11月10日24:00前，将实验报告发送到陈泽茂老师的电子邮箱chenzemao@whu.edu.cn，邮件主题为“软件安全实验三”。