设计内容要求

1. 结合课堂所讲授的内容，围绕着“**Windows 自启动项的查看和分析**”主题，查阅课外资料，编写验证代码，动手进行实验，撰写一份技术研究和设计开发报告，要求有一定深度的分析和实践步骤，主题明确，条理清晰，文字流畅，图文并茂，字数不限。此外，还需一并附上可执行软件和源代码。

2. 可以参考 SysinternalsSuite 工具集中的 Autoruns 软件，了解在 Windows 系统中有哪些可以实现自启动的技术方法，然后分析它们各自的技术原理、实现细节和隐蔽性状况，撰写到课程报告之中。

所研究和分析的自启动种类必须包括以下这些：

- Logon：启动目录，基于注册表启动；
- Services：系统服务；
- Drivers：系统驱动程序；
- Scheduled Tasks：计划任务。

此外，还可以研究和分析以下这些：

- Internet Explorer：IE 浏览器的 BHO 对象；
- Boot Execute：启动执行；
- Image Hijacks：映像劫持；
- Known DLLs：知名动态链接库；
- Winsock Providers：Winsock 服务提供程序
- Winlogon：用户登录通知程序
- …….

3. 编写自己的 Windows 自启动项查看软件。

- Windows 系统版本为：Windows 7 企业版/专业版 SP1，64 位；
  安装 ISO 文件链接：https://jbox.sjtu.edu.cn/l/MFKIPD （提取码：ctrk）
- 基本功能必须实现，可选功能不限；
- 开发语言限定为 C/C++/C#，不能使用 Python、Java、Perl、VB 等。

报告提交要求

1. 每份研究报告由每位同学独立撰写完成，完成后将研究报告，实现代码以及可执行文件一并压缩打包上传。压缩文件格式为：

学号_姓名.rar/.zip/.7z

2. 提交截止时间：

2021 年 6 月 13 日

3. 提交方式：

- ftp://ericwyj:public@public.sjtu.edu.cn/upload/IS/windows_security/

评分标准

总分 20 分，标准如下：

1）报告完整且原创 8 分

2）代码完整且原创 2 分

3）基本的功能实现

- Logon：启动目录，注册表启动 4 分
- Services：系统服务 2 分
- Drivers：系统驱动程序 2 分
- Scheduled Tasks：计划任务 2 分

4）可选的功能实现

每项各 1 分，但总分加起来不超过 20 分

- Internet Explorer：IE 浏览器的 BHO 对象
- Boot Execute：启动执行
- Image Hijacks：映像劫持
- Known DLLs：知名动态链接库
- Winsock Providers：Winsock 服务提供程序
- Winlogon：用户登录通知程序
- ……