“网络与信息安全”2023 年春大作业

1. 提交方式

该作业需要**编写程序**并**完成报告**，其中，报告限长度**不超过** 8 页。

提交：请在作业截止前发送**程序代码**（压缩包）和**技术报告**（pdf）到 zhran_bit@126.com。

作业截止：**2023 年 5 月 21 日（周日）晚 23 点 59 分**。（**请务必准时提交！**）

文件命名要求：教室名-作业方向名称-学号-姓名

- 例：综 A102-缓冲区溢出及漏洞利用方向-123456789-张三.zip (.pdf)
- 例：文 B130-人工智能安全方向-987654321-李四.zip (.pdf)

2. 作业内容

选择以下八个方向之一，不鼓励八个方向外的选题，具体题目自拟，**必须**涉及编程或程序配置，代码行数**不少于 100 行**。各方向每项参考内容均与作业内容体量相当。

社会工程学攻击方向

以下为参考内容，建议结合兴趣自拟内容：

（1） 选择一款社会工程学工具，尝试在合法范围内使用，并形成记录；或

（2） 优化修改一款社会工程学工具；

缓冲区溢出及漏洞利用方向

以下为参考内容，建议结合兴趣自拟内容：

（1） 选择一个公开发布的漏洞，参考资料编制漏洞利用程序，形成分析报告；或

（2） 编写已知公开漏洞的利用脚本；或

（3） 结合缓冲区溢出原理，编写程序及文档进行详细讲解；

Web 安全及 SQL 注入方向

以下为参考内容，建议结合兴趣自拟内容：

（1） 在合法范围内，实施一次跨站脚本攻击（可自搭建目标机器），形成分析报告；或

（2） 在合法范围内，实施一次 SQL 注入攻击（可自搭建目标机器），形成分析报告；或

（3） 在合法范围内，实施一次与 Web 安全相关的攻击，形成分析报告。

安全隐蔽通信方向

以下为参考内容，建议结合兴趣自拟内容：

（1） 以数据安全回传为目标，设计一种传输方法，编写程序实现；或

（2） 以隐蔽发送方为目标，设计一种传输方法，编写程序实现；或

（3） 以隐蔽接收方为目标，设计一种传输方法，编写程序实现；或

（4） 自主搭建跨越洲通信的 VPN 服务，并编写配置脚本；或

（5） 配置洋葱路由器（Onion Router），实现逆踪访问。

安全工具软件实践方向

以下为参考内容，建议结合兴趣自拟内容：

（1） 选择一款安全工具软件，实践一个较复杂功能，编写配置脚本，形成分析报告；或

（2） 选择一个安全工具网站，实践一个较复杂应用，编写配置脚本，形成分析报告。

人工智能安全方向

以下为参考内容，建议结合兴趣自拟内容：

（1） 部署 DeepFake，利用人工智能进行冒用身份攻击的技术实践；或

（2） 用人工智能方法解决某个网络安全问题，适度编程，形成技术分析报告。

移动 APP 安全方向

以下为参考内容，建议结合兴趣自拟内容：

（1） 挖掘某个手机 APP 的安全问题，开展技术实践，形成技术分析报告；或

（2） 采用抓包等方式，分析 5G 移动网络的计费及通信模式，形成技术分析报告。

多模态大模型安全方向

以下为参考内容，建议结合兴趣自拟内容：

（1） 基于 ChatGPT/文心一言/其他大语言模型，设计 Prompt 对话，诱导其生成可执行网络攻击及防御配置脚本（需验证），开展技术实践，形成技术分析报告；或

（2） 基于 ChatGPT/文心一言/其他大语言模型，设计 Prompt 对话进行漏洞分析，并尝试利用该漏洞进行攻击，开展技术实践，形成技术分析报告；或

（3） 基于 ChatGPT/文心一言/其他大语言模型，根据所提供的接口进行程序开发，实现基于大模型的叠加功能，解决大模型难以解决的问题，形成技术分析报告。

3. 总体说明

作业所编写代码规模最低不少于 100 行，配置参数及选取相当，编程语言不限；对于操作、应用及配置类作业，所完成实践的复杂性不低于编写 100 行代码规模的难度。

注意：100 行规模参考 Python 语言规模，非 C 语言 100 行规模。

作业成绩评判标准依次为：创新性、完成度、报告质量、新编制代码行数、代码质量、个人工作量等。

大作业占总成绩 30 分。