课程设计要求

一. 课程设计的题目

可从以下多个题目中任选一个题目，完成课程设计。

题目 1：基于智能算法的网络加密流量中木马后门检测技术

在多种操作系统中，构建多种类型高隐藏木马后门的运行环境，通过收集或捕获运行环境目标计算机木马后门发出的网络加密数据包，通过样本分析，设计完成基于指纹识别、模型匹配以及智能算法识别的方法，实现对不同类别木马后门，可检测分析出加密网络数据包中的恶意木马后门数据包及其恶意行为分类，分析木马后门检测的准确率和误报率。

测试环境：

Windows 或 Linux 操作系统计算机，安装所开发的基于机器学习和样本特征的加密网络流量木马后门行为检测工具，可捕获离线或在线的木马后门行为数据包，并进行其木马后门行为检测分析分类，最后分析出检测的准确率和误报率。自己构建多类木马后门环境，捕获木马后门的网络数据包，自己分析特征。

提示：

学习网络协议解析；

学习机器学习等智能化检测算法；

学习高隐藏后门行为的典型特征。

评分要点：

支持可检测的高隐藏性木马后门的类型、行为、特征的多少，以及检测方法丰富性，检测准确性、误报率、漏报率。

题目 2：云原生/大数据开源软件代码中木马后门检测

针对云原生、大数据、智能模型开源项目中，对使用 JAVA、Python、Go 语言的开源软件或组件源代码，检测代码中是否隐藏存在多类型的木马后门，造成安装此类开源软件源代码并运行后，导致计算机被攻击被控制和信息外泄。

注：不能使用开源软件实现此题目。

测试环境：

Windows 或 Linux 操作系统计算机，安装所开发的开源软件源代码后门木马检测工具，检测源代码中隐藏的多种类型后门木马等恶意代码，并形成检测报告，分析准确率和误报

率。

提示：

学习后门木马等恶意软件代码在代码上的表现形式；

学习模式匹配、中间语言转换、向量转换等源代码检测技术。

评分要点：

覆盖的语言、木马后门的种类、检测方法的丰富性。

题目 3：移动终端鸿蒙系统的安全缺陷漏洞扫描检测工具

为了提高开源鸿蒙系统的安全性，开发鸿蒙系统安全漏洞的扫描和检测工具。可对鸿蒙系统的 app 漏洞、网络服务漏洞、系统漏洞进行漏洞安全扫描和检测，检测应用软件、系统软件、网络服务的漏洞，可以以自定义的标准输出模板显示检测的结果，按照漏洞的危险级别和数量进行统计并显示，能定位漏洞信息，给出漏洞的验证和修复方法。

测试环境：

自己搭建鸿蒙系统的真实或模拟器环境，利用开发的安全漏洞扫描工具，检测相关安全缺陷或漏洞，并形成漏洞扫描报告。对扫描出的漏洞进行漏洞可利用性或危害验证，定位漏洞的代码点，提出修复的方法。

提示：

学习鸿蒙系统的构建

学习鸿蒙系统的开发

学习鸿蒙系统漏洞的原理

学习鸿蒙系统漏洞的扫描检测技术和漏洞利用验证技术

评分要点：

支持的安全漏洞检测类型，覆盖的软件或服务的丰富程度，对漏洞的可利用性验证和修复的效果。

题目 4：主机系统的持久驻留和多通道隐蔽回传技术

为了检测高隐藏性恶意程序，有必要深入学习和了解高隐藏性木马后门在主机系统中的持久性驻留技术，以及高隐藏性多通道回传技术。开发针对 linux 的特定程序，在支持简单远控木马功能条件下，具备高隐藏性持久化驻留功能，在主流杀毒软件安装条件下，可实现支持开机正常启动和运行过程中的免杀。此外，具备多通道隐蔽回传功能，实现利用社交

网络等多种常见网络传输通道实现隐蔽信息的加密回传，以及多通道回传信息的汇聚重组功能。

测试环境：

在 Linux 环境和安装主流杀毒软件条件下，通过开发的特定恶意程序，实现支持 linux 开机时的正常启动和运行过程中的免杀，支持多通道信息回传和回传后接收节点的汇聚重组功能。

提示：

学习 Linux 的引导流程

学习 Linux 中杀毒软件的机理

学习绕过杀毒软件/EDR 软件的方法

学习常用网络传输通道的模仿和注入类传输技术

评分要点：

支持的持久化驻留方法、绕过杀毒软件的免杀方法、高隐藏性多通道回传方法和重组功能实现完备性。

二、课程设计组队方法

班内班间自由组合，每个题目最多 12 人组成开发小组，合作完成。

在任务分工文件中详细描述各个成员的分工，以及相应的工作量占比。

三、课程设计考核方式

打包提交任务分工说明、作品技术原理介绍、概要设计报告、详细设计报告、测试分析报告、程序编译和安装使用文档、程序源代码、ppt、截屏录像。包命名方式：组长班级+组长姓名+学号.rar/ZIP

各班学委将分组表汇总到大班学委，大班学委将分组表发到 email：yuanjie@bupt.edu.cn 和 cuibj@bupt.edu.cn 中，包括分组序号、所选题目号、组长（留手机号）和组员的学号和姓名、班号，按照班号由小到大排序，答辩顺序按照组长学号顺序由小到大答辩。

9 月 6 日验收考核，地点沙河校区 S118，每组进行 15 分钟的 ppt 介绍和作品演示（每组限制时间），提前到教室来试好演示环境。考核的顺序：按照班号由小到大排序，每个班按照组长的学号由小到大为顺序先后介绍。上午 8：00－12：00，下午 1：00－全部答辩完。

按照老师意见修改并完成报告和提交材料，下午 18 点前提交报告至 email：

yuanjie@bupt.edu.cn。

根据小组提交程序的完成情况、完成的功能、稳定性、存在问题的多少、文档及报告完成情况、技术的合理性、技术的难度和自主性、程序的开发工作量等给予打分。

建议要求同学提前一天自行去教室测试环境和设备，保证验收时的正常演示。

四、授课老师联系方式

崔宝江 13611330827　苑洁 18911815861

该二维码7天内(9月6日前)有效，重新进入将更新