广州大学
GUANGZHOU UNIVERSITY

博学笃行 与时俱进

网络空间安全综合实验

2023.03

主要内容

一、课程总体情况

二、课程实验主题方向

三、课程要求

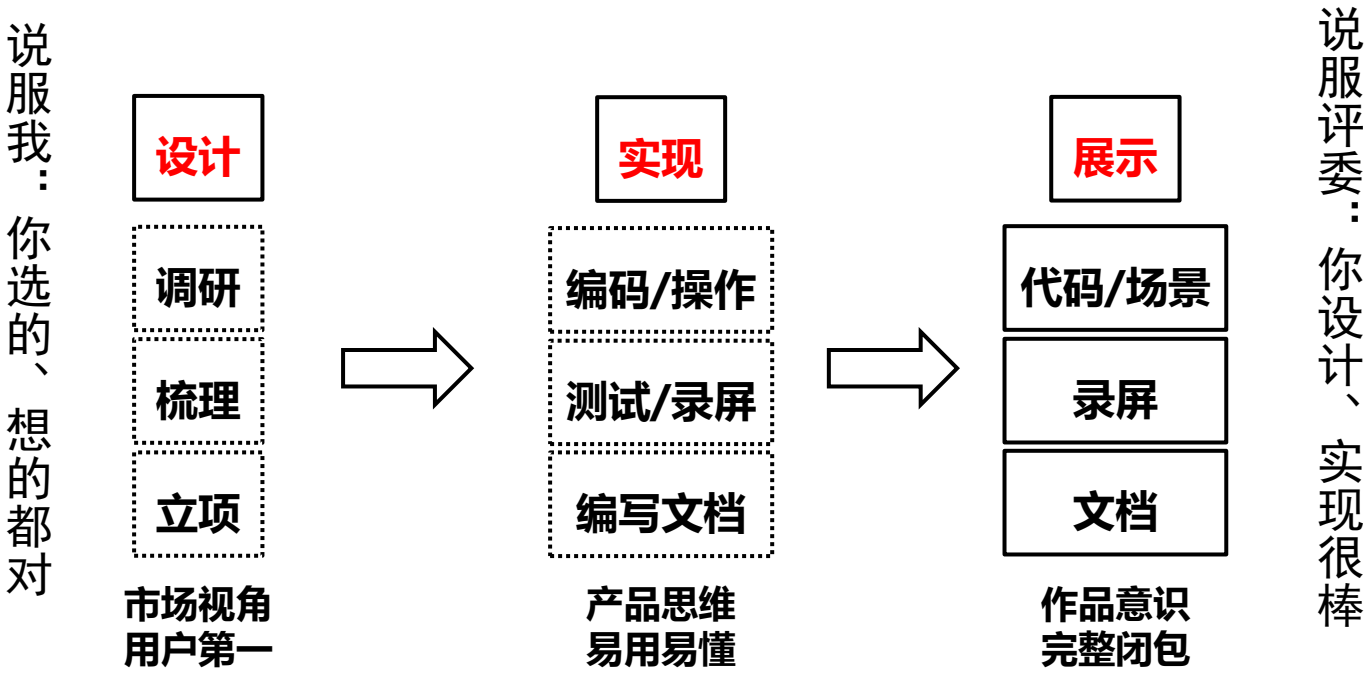
四、时间安排

一、课程总体情况

课程目的

- ✓ 对前期理论课、导论课、研讨课（汇报）课、实验实践课等的总结和运用
- ✓ 通过实践，熟悉转换角色/视角的思维方法、设计方法，演示实现方法
- ✓ 市场视角、产品思维、作品意识

课程形式



主要内容

一、课程总体情况

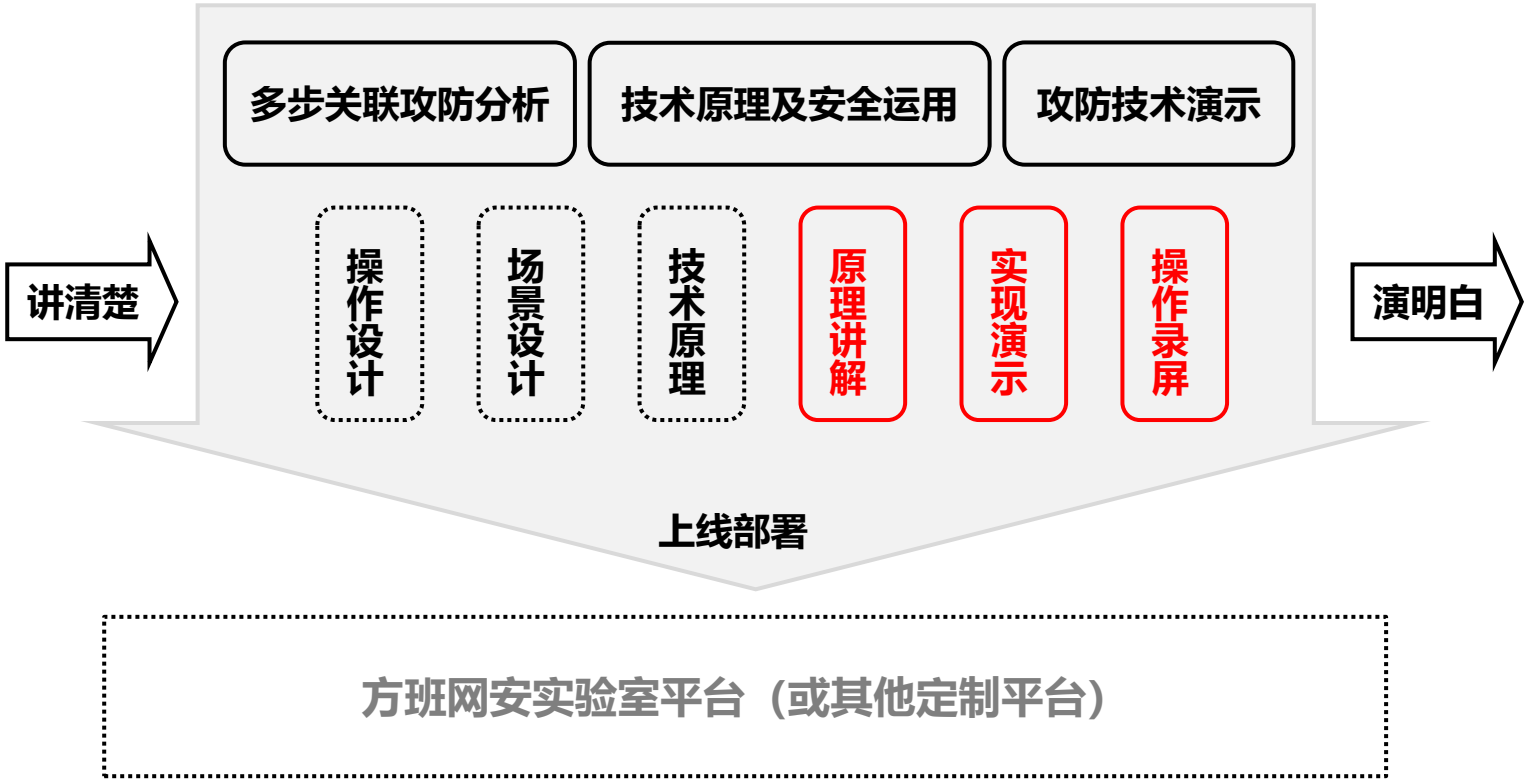
二、课程实验主题方向

三、课程要求

四、时间安排

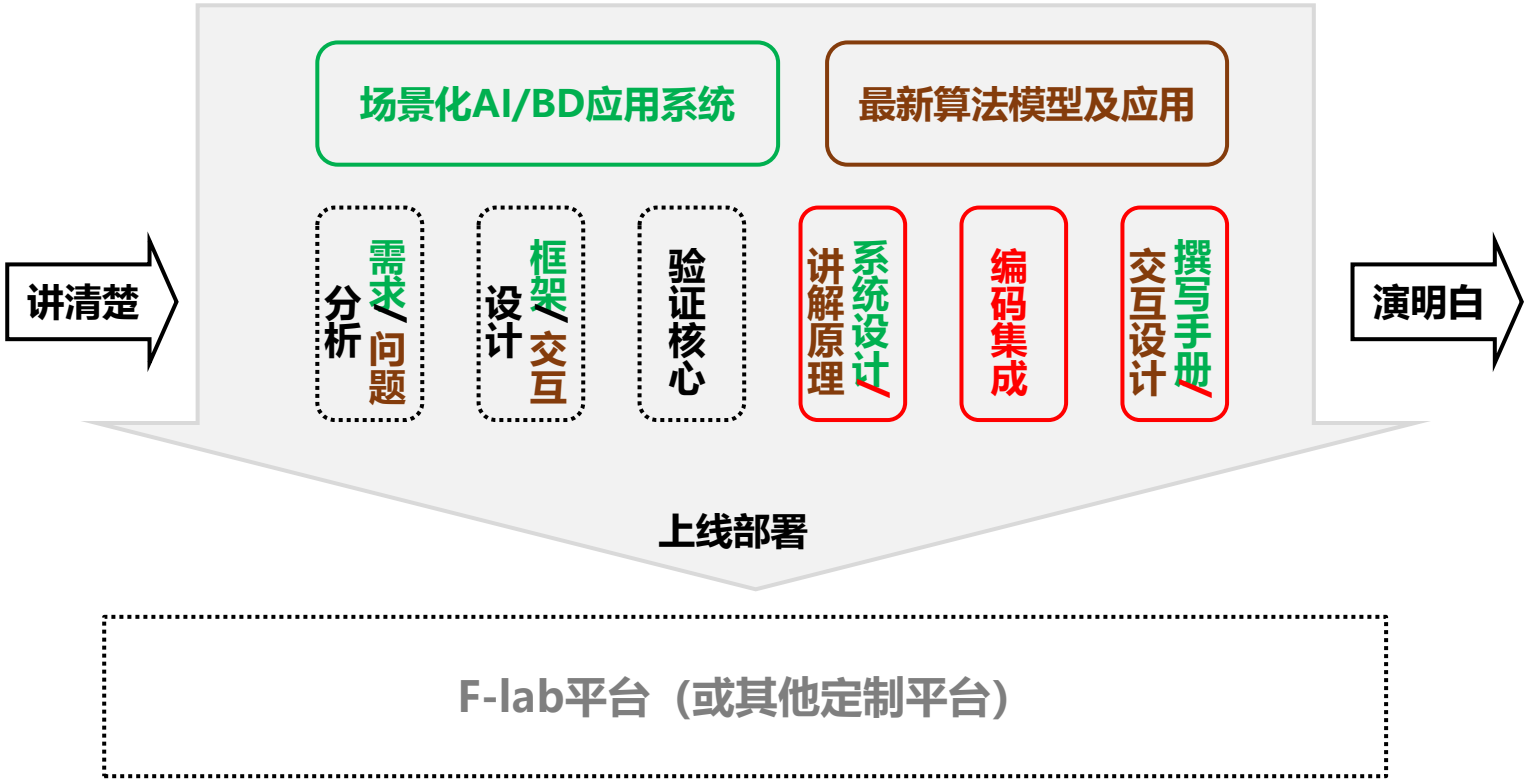
二、课程实验的主题方向

□ 网络与系统（软件）安全



二、课程实验的主题方向

□ 人工智能/大数据技术与安全



主要内容

一、课程总体情况

二、课程实验主题方向

三、课程要求

四、时间安排

三、课程要求-过程

设计先行

- ✓ 设想：选题目、选事件、选漏洞，选主题、选方向、选平台（工具）
- ✓ 设计：环境设计、样式设计、内容设计，功能设计、流程设计、交互设计

审核把关

- ✓ 设计**审核通过**后，才能登记题目题目
- ✓ 登记的题目作品**验收通过**后，才算完成

以该文档记录为准

题目登记及评分表

（腾讯文档）

实施要求

- ✓ ≤ 2人/组(中间不允许换组)
- ✓ 严格按时间节点“交付”
- ✓ 严格遵守格式样式要求
- ✓ 注重换位换视角思考
- ✓ “作品”与“作业”的区别
- ✓ 体现产品和作品的可展示性

三、课程要求-审题

网安类

1.理论大纲（至少到二级）
2.实验大纲（至少到二级）
3.工具列表（分析工具、环境工具，名称和版本）
4.目的和预期效果（文字描述）

场景化应用系统类

1.需求分析（文字）
2.功能流程设计（业务需求视角，文字+图）
3.结构设计（顶天立地模块结构图，数据流图及格式）
4.运行部署环境设计（图+文字）
5.技术重难点及依据（表格）

模型算法及应用类

1.理论大纲（至少到二级）
2.数据集简单统计特征（表-指标及数字）
3.算法可调/交互/干预参数（表-参数及含义作用）
4.运行结果展现形式设计（图+注释文字）
5.人机交互和运行干预界面设计（图+注释文字）

报名审题前，逐字逐项理解和对照检查自己的设计。
与授课老师现场确认并在在线登记表格登记后方可作为候选作品。

三、课程要求-验收

□ 网安类

1.理论部分

0：无理论讲解或讲解不足页

3：有图有例有层次，与实验内容基本对应

5：教科书级理论内容，由浅入深，层层相扣，紧贴实验内容，图和例切题

2.实验部分

0：无实验或实验未完成，或内容少于10个操作步

3：实验步骤内容清晰，步骤连贯，输入输出有注释和讲解

5：在以上基础上，分析步骤间的联系，解释前后步骤的因果关系

验收项目

1 实验指导书，放在实验目录下，文件命名为“实验指导书.docx”

2 录屏视频，放在实验目录下，文件命名为“录屏.mp4”

3 完整的虚拟机环境/镜像文件，文件名为“操作系统名-版本.qcow2”

4 详细拓扑环境配置信息（readme.txt）

报名验收前，逐字逐项理解和对照检查自己的作品。

三、课程要求-验收

□ 场景化应用系统类

1.中期（0.3）

0：无设计或设计资料不完整

3：功能流程、模块结构、数据流及交互等设计完整

5：开发环境部署完整，核心代码可运行

2.最终（0.7）

0：设计功能完成度不足半或无法运行

3：完成主要功能，设计文档（包括但不限于功能、结构、模块、交互等部分）完整

5：功能完整、运行流畅，编码规范，设计文档规范合理，安装使用文档清晰完整

验收项目

1 设计文档（功能、结构、模块、交互等四种文档），文件命名为“系统设计.docx”

2 安装使用手册，文件命名格式为“安装使用手册.docx”

3 程序运行及功能介绍录屏，文件命名格式为“录屏.mp4”

4 源代码，按照开发编译所要求的子目录结构

5 详细的开发及运行环境软硬件配置信息（readme.txt）

报名验收前，逐字逐项理解和对照检查自己的作品。

三、课程要求-验收

□ 模型算法类

1.理论部分

0：无理论讲解或讲解不足页

3：有图有例有层次，与实验内容基本对应

5：教科书级理论内容，由浅入深，层层相扣，紧贴实验内容，图和例切题

2.代码部分

0：无代码或代码未完成或核心部分调库

3：程序结果正确，编码较为规范，可调参数有效（避免黑盒化）

5：可调参数丰富（算法原始输入之外的参数）、人机交互友好；编码规范

验收项目

1 实验指导书，放在实验目录下，文件命名格式“实验指导书.docx”

2 程序运行及功能介绍录屏，文件命名为“录屏.mp4”

3 源代码，按照开发编译所要求的子目录结构

4 详细的开发及运行环境软硬件配置信息（readme.txt）

报名验收前，逐字逐项理解和对照检查自己的作品。

三、课程要求-考核

考核单元

- ✓ 网安类：多步关联攻防分析 —— 4层以上网络，5种以上关联攻防方法/操作
  技术原理及安全运用 —— 每个实验满分20分
  攻防技术演示 —— 每个实验满分20分
- ✓ 应用类：按功能模块，具体在审题时确定功能和样式要求
- ✓ 算法类：模型算法应用 —— 每个实验满分20分

考核形式

- ✓ 按组考核，⩽2人/组
- ✓ 1名授课老师，2名学生志愿者；根据统一标准独立打分，求平均
- ✓ 随课程分4个考核节点，包括实验指导书/设计手册、录屏
- ✓ 成绩实时公布在腾讯文档的表格上，主动关注自己的审题、验收和考核评分

主要内容

一、课程总体情况

二、课程实验主题方向

三、课程要求

四、时间安排

四、时间安排

第 二 学 期（二十周）									
月份	周次	星期							摘 要 事 项
		日	一	二	三	四	五	六	
二	一	19	20	21	22	23	24	25	上课：2月20日
	二	26	27	28					
三					1	2	3	4	
	三	5	6	7	8	9	10	11	
	四	12	13	14	15	16	17	18	
	五	19	20	21	22	23	24	25	
	六	26	27	28	29	30	31		
四								1	
	七	2	3	4	5	6	7	8	清明节：4月5日放假
	八	9	10	11	12	13	14	15	
	九	16	17	18	19	20	21	22	
	十	23	24	25	26	27	28	29	
	十一	30							
五			1	2	3	4	5	6	劳动节：4月29日至5月1日放假
	十二	7	8	9	10	11	12	13	
	十三	14	15	16	17	18	19	20	
	十四	21	22	23	24	25	26	27	
	十五	28	29	30	31				
六						1	2	3	
	十六	4	5	6	7	8	9	10	
	十七	11	12	13	14	15	16	17	
	十八	18	19	20	21	22	23	24	端午节：6月22-24日放假. 学位会6月20日
	十九	25	26	27	28	29	30		毕业生离校：6月28日-30日
七								1	19-20周为考试周
	二十	2	3	4	5	6	7	8	
	暑假	9	10	11	12	13	14	15	学生暑假：7月8日至8月27日

验收课

审题/辅导课

小结

三、课程要求-过程

设计先行

- ✓ 设想：选题目、选事件、选漏洞，选主题、选方向、选平台（工具）
- ✓ 设计：环境设计、样式设计、内容设计，功能设计、流程设计、交互设计

审核把关

- ✓ 设计审核通过后，才能登记题目题目
- ✓ 登记的题目作品验收通过后，才算完成

以该文档记录为准

题目登记及评分表（腾讯文档）

实施要求

- ✓ ≤ 2人/组(中间不允许换组)
- ✓ 严格按时间节点“交付”
- ✓ 严格遵守格式样式要求
- ✓ 注重换位换视角思考
- ✓ “作品”与“作业”的区别
- ✓ 体现产品和作品的可展示性

审题 → 。。。实现/辅导。。。 → 验收

三、课程要求-审题

网安类

1.理论大纲（至少到二级）
2.实验大纲（至少到二级）
3.工具列表（分析工具、环境工具，名称和版本）
4.目的和预期效果（文字描述）

场景化应用系统类

1.需求分析（文字）
2.功能流程设计（业务需求视角，文字+图）
3.结构设计（顶天立地模块结构图，数据流图及格式）
4.运行部署环境设计（图+文字）
5.技术重难点及依据（表格）

模型算法及应用类

1.理论大纲（至少到二级）
2.数据集简单统计特征（表-指标及数字）
3.算法可调/交互/干预参数（表-参数及含义作用）
4.运行结果展现形式设计（图+注释文字）
5.人机交互和运行干预界面设计（图+注释文字）

报名审题前，逐字逐项理解和对照检查自己的设计。
与授课老师现场确认并在在线登记表格登记后方可作为候选作品。

三、课程要求-验收

网安类

1.理论部分
- 0：无理论讲解或讲解不足页
- 3：有图有例有层次，与实验内容基本对应
- 5：教科书级理论内容，由浅入深，层层相扣，紧贴实验内容，图和例切题

2.实验部分
- 0：无实验或实验未完成，或内容少于10个操作步
- 3：实验步骤内容清晰，步骤连贯，输入输出有注释和讲解
- 5：在以上基础上，分析步骤间的联系，解释前后步骤的因果关系

验收项目
1 实验指导书，放在实验目录下，文件命名为“实验指导书.docx”
2 录屏视频，放在实验目录下，文件命名为“录屏.mp4”
3 完整的虚拟机环境/镜像文件
4 详细拓扑环境配置信息（readme.txt）

场景化应用系统类

1.中期（0.3）
- 0：无设计或设计资料不完整
- 3：功能流程、模块结构、数据流及交互等设计完整
- 5：开发环境部署完整，核心代码可运行

2.最终（0.7）
- 0：设计功能完成度不足半或无法运行
- 3：完成主要功能，设计文档（包括但不限于功能、结构、模块、交互等部分）完整
- 5：功能完整、运行流畅，编码规范 设计文档规范合理，安装使用文档清晰完整

验收项目
1 设计文档（功能、结构、模块、交互等四种文档），文件命名为“系统设计.docx”
2 安装使用手册，文件命名格式为“安装使用手册.docx”
3 程序运行及功能介绍录屏，文件命名格式为“录屏.mp4”
4 源代码，按照开发编译所要求的子目录结构
5 详细的开发及运行环境软硬件配置信息（readme.txt）

模型算法类

1.理论部分
- 0：无理论讲解或讲解不足页
- 3：有图有例有层次，与实验内容基本对应
- 5：教科书级理论内容，由浅入深，层层相扣，紧贴实验内容，图和例切题

2.代码部分
- 0：无代码或代码未完成或核心部分调库
- 3：程序结果正确，编码较为规范，可调参数有效（避免黑盒化）
- 5：可调参数丰富（算法原始输入之外的参数）、人机交互友好；编码规范

验收项目
1 实验指导书，放在实验目录下，文件命名格式“实验指导书.docx”
2 程序运行及功能介绍录屏，文件命名为“录屏.mp4”
3 源代码，按照开发编译所要求的子目录结构
4 详细的开发及运行环境软硬件配置信息（readme.txt）

报名验收前，逐字逐项理解和对照检查自己的作品。

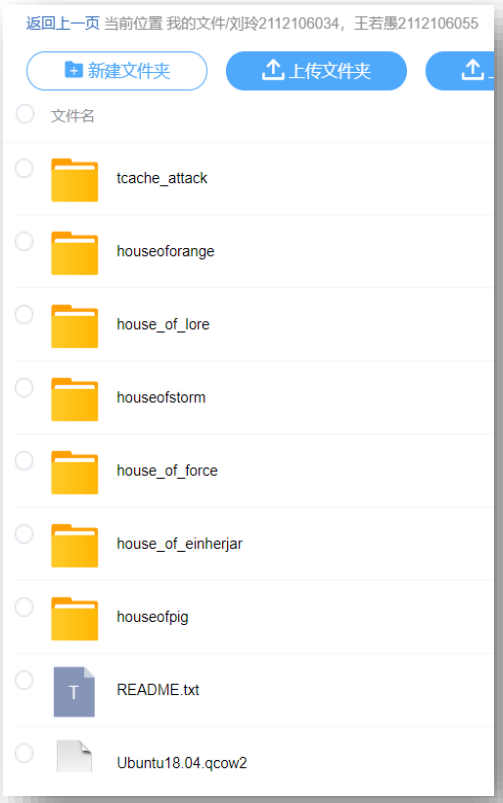
作业作品提交

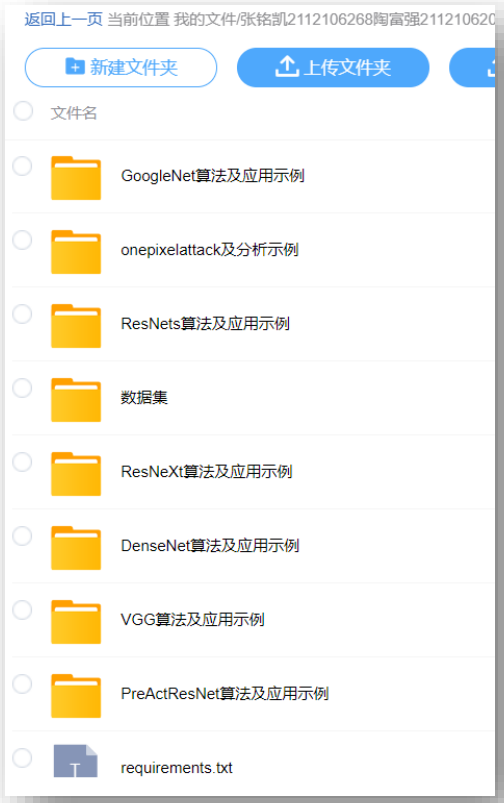
浏览器访问：http://172.22.105.161

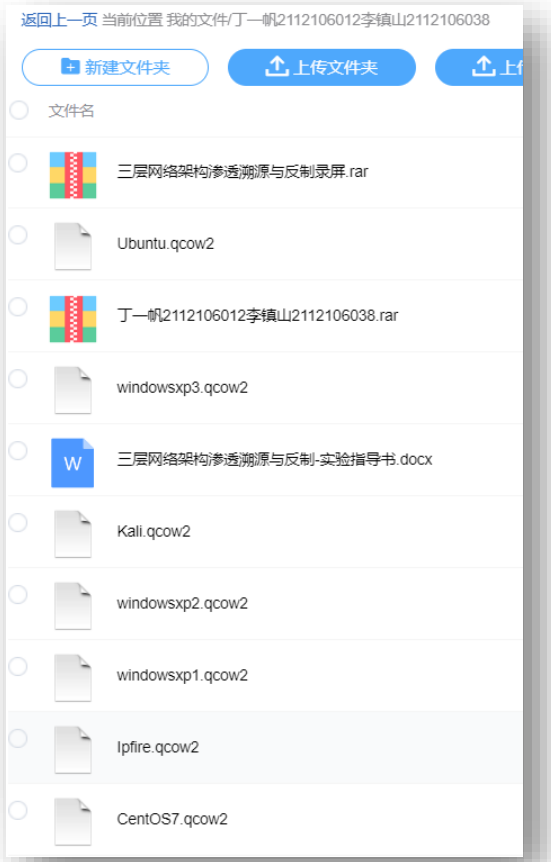
账号/密码：zhsy5/zhsy5!

注：校内可直接访问，校外需用广州大学vpn；单个文件不超过4GB

作业作品样例







1.同类型攻防系列　　**2.同类型算法系列**　　**3.多层系列关联攻击**

提供一个直观的印象，不代表以上就是最好的或唯一的，而实际上它们也有不足。

推荐题目

一、网安类

1. 四层以上场景靶标及对应渗透实验
2. 基于杀伤链模型的场景化演示（杀伤链原理与场景构建、前5选4后2合1，共5个）
3. 基于钻石模型的场景化攻击演示/复现（4层以上场景靶标、5步以上攻击链）
4. 基于ATT_CK的场景化攻击演示/复现（4层以上场景靶标、5步以上攻击链）
5. 白皮书体系（定位在二级标题成系列）

二、应用类

1. Flex、Bison、LLVM实验
2. PE、ELF深度分析工具（面向异常检测，例如恶意代码-静态或恶意行为-动态）
3. 数据标注工具（不同类型数据——典型类型和结构的数据）
4. 智能的网络/主机入侵检测工具（采集、预处理、计算/训练、人机交互的完整部分）

编码规范——**标识符**（命名易读易理解）

模块化（模块-文件-函数-嵌套-语句）

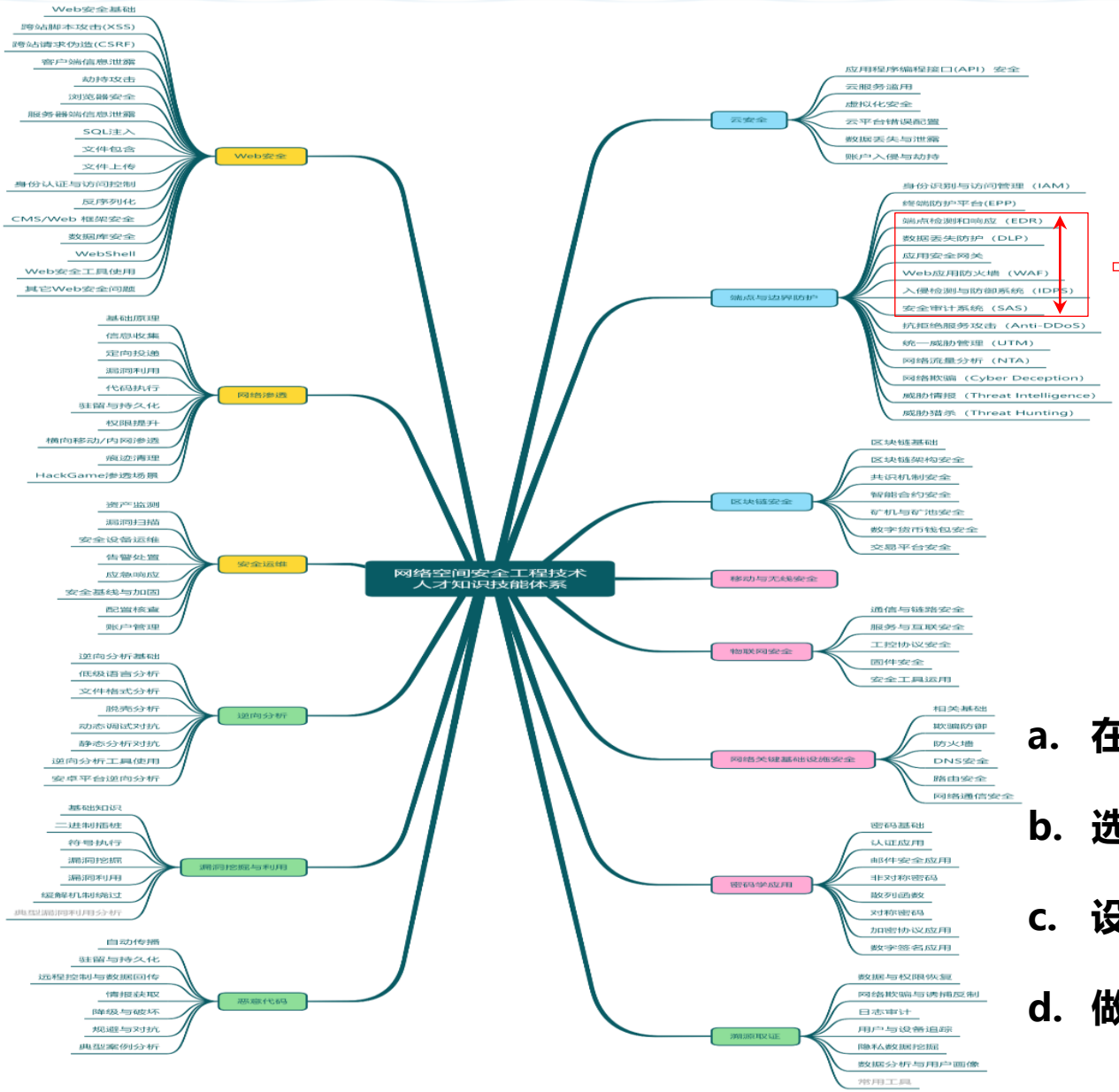
注释（一“句”一注释，一符一注释）

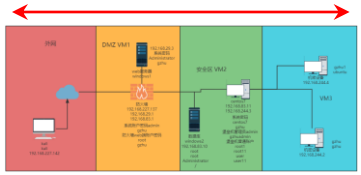
缩进与空行空格

- https://zh-google-styleguide.readthedocs.io/en/latest/contents/

模拟器 —— SEED Emulator https://seedsecuritylabs.org/emulator/

方班技能白皮书-一种构思实验题目的思路





王小明的抡大锤实验：
1.收集信息
2.设计payload
3.钓鱼攻击/渗透攻击
4.漏洞利用
5.驻留/横移
6.建立CC通道/获取数据

a. 在一个二级节点下

b. 选几个上下相关的主题

c. 设计一个**集成化**的场景

d. 做一组**前后关联**的攻防

Q & A