《信息安全综合实践》

课程教学大纲

一、 课程基本信息

课程类型	专业必须课	□理论课（含上机、实验学时）			
		□实习 ☑课程设计 □毕业设计			
课程编码	7262711	总学时	5 周	学分	5
课程名称	信息安全综合实践				
课程英文名称	Integrated practical training of information Security				
适用专业	信息安全				
先修课程	（7240911）信息安全、（7232701）软件安全、（7237611）网络攻击与防御、（7235621）数字取证				
开课部门	信息学院计算机系				

二、 课程性质与目标

《信息安全综合实践》本课程的授课对象为信息安全专业，课程属性为专业必修课。课程主要用于提升学生对信息安全知识的综合运用能力和加深对相关信息安全工具的灵活掌握。通过对信息安全知识综合运用能力的锻炼，提升学生对信息安全知识的灵活运用、分析安全问题、解决安全问题的能力。

通过本课程学习，学生能够达到

课程目标 1：综合运用所学安全知识解决问题

课程目标 2：发现所学知识与实际应用需求之间的差距并针对性的加强学习

课程思政目标：树立保护我国网络空间安全的意识和提升相应技能，同时提高学生法律意识、加强品德修养，坚定学生理想信念、厚植爱国主义情怀。

三、 课程教学基本内容与要求

1. 经典漏洞的复现分析实验

通过对经典漏洞的复现和分析，让学生掌握漏洞分析的方法和挖掘漏洞产生的原因，推荐学生可选如下内容（但不限于）

1	栈溢出漏洞分析（不限于）： CVE-2010-2883、CVE-2010-3333
2	堆溢出漏洞分析（不限于）：CVE-2010-2553、CVE-2012-0003
3	整数溢出漏洞分析（不限于）：CVE-2011-0027、CVE-2012-0774
4	格式化字符串漏洞分析（不限于）：CVE-2012-0809、CVE-2012-3569

5	其他类型经典漏洞复现

考核形式：验机（至少完成 3 个漏洞复现并提交实战报告）

2. CTF 解题并提交相应的 flag 实验

采用 CTF 题目模式，加速学生提升综合运用所学知识能力

1	MISC 类型，涉及流量分析、电子取证、人肉搜索、数据分析
2	CRYPTO 类型，涉及各种加解密技术，包括古典加密技术、现代加密技术
3	PWN 类型，涉及文件的漏洞发现与利用
4	STEGA 类型，将目标会隐藏到图片、音频、视频等各类数据载体中。
5	REVERSE 类型，即逆向工程，涉及到软件逆向、破解技术
6	WEB 类型，涉及到常见的 Web 漏洞，诸如注入、XSS、文件包含等漏洞

考核形式：验机（至少完成 3 个 CTF 解题实战并提交实战报告）

注：本课程不提供攻击环境与攻击工具，需学生自己下载。在课程期间，学生尽可能多的提交漏洞分析报告及尽可能多的攻陷靶场系统并提交攻击报告。

四、 实践性教学内容的安排与要求

为了加强学生对信息安全知识综合运用能力，将理论和实际应用切实结合起来。本课程全部采用实践教学方式完成，在专业实验室统一做实验和验收，并按时提交实践报告。

五、 教学设计与教学组织

第 1 部分经典漏洞的复现分析实验内容选取教材中展示的经典 CVE 进行复现，但不限制且鼓励学生复现除此来源之外的其他漏洞；第 2 部分 CTF 解题可选取教材及参考资料中的赛题进行实战，也可以选取之外的其他网络来源 CTF 赛题进行实战。对于学生的任何选题来源持鼓励态度，目标都是提升学生综合运用所学知识的能力，以期培养合格的保卫我国网络空间领空安全的人才。

六、 教材与参考资料

1.教材

（1）《漏洞战争》，林桠泉等著，电子工业出版社，2016 年，ISBN：9787121289804

（2）《CTF 特训营：技术详解、解题方法与竞赛技巧》，FlappyPig 战队著，机械工业出版社，2020 年，ISBN：787111657354

2.参考资料

（1）《论网络空间主权》（第 1 版），方滨兴著，科学出版社，2020 年，ISBN：9787030542557

七、 课程考核方式与成绩评定标准

采用百分制，总评成绩由平时成绩、实践教学报告成绩两部分组成，平时成绩占 30%，实践报告成绩占 70%。

八、 大纲制(修)订说明

无

大纲执笔人：杜春来
大纲审核人：李琛
开课系主任：肖珂
开课学院教学副院长：宋威
制（修）订日期：2022 年 2 月