【网络攻防技术】

【Hacking and Defence】

一、基本信息

课程代码：【2058090】
课程学分：【2 】
面向专业：【全校公选课】
课程性质：【公选课】
开课院系：【信息技术学院物联网工程系】
使用教材：
教材【自编教材】
参考书目【网络安全实践教程（第二版），王磊，铁道出版社，2023.4】
【信息安全攻防实用教程，马洪连，机械工业出版社，2014.4】
课程网站网址：【超星平台】等
先修课程：【计算机网络原理】

二、课程简介

本课程主要讲解网络安全的基本操作技能，并结合 CTF 大赛，说明相关的密码学，渗透学，隐写技术，漏洞挖掘技术，WEB 渗透技术，取证技术等相关内容，课程以实践为主，注重操作技能的培养。

三、选课建议

本课程是适用于全校所有本科学生，要求学生具有一定的计算机网络原理基础知识。

四、课程与专业毕业要求的关联性

毕业要求	关联
LO1：工程知识：能够将数学、自然科学、工程基础和专业知识用于解决复杂工程问题	
LO23：能够对复杂工程问题进行分析和求解，并能通过文献研究或实验寻找可替代的解决方案。	●
L03：设计/开发解决方案：能够设计针对复杂工程问题的解决方案，设计满足特定需求的系统、单元（部件）或工艺流程，并能够在设计环节中体现创新意识，考虑社会、健康、安全、法律、文化以及环境等因素	
L04: 研究：能够基于科学原理并采用科学方法对复杂工程问题进行研究，包括设计实验、分析与解释数据、并通过信息综合得到合理有效的结论	
LO52：能够针对复杂物联网工程问题，选择恰当的虚拟仿真工具或方法，对系统或其解决方案进行必要的模拟与预测，并能够理解仿真模拟系统与真实系统之间的差异。	●
L06: 工程与社会：能够基于工程相关背景知识进行合理分析，评价专业工程实践和复杂工程问题解决方案对社会、健康、安全、法律以及文化	

的影响，并理解应承担的责任	
L07: 环境和可持续发展：能够理解和评价针对复杂工程问题的专业工程实践对环境、社会可持续发展的影响	
L08: 职业规范：具有人文社会科学素养、社会责任感，能够在工程实践中理解并遵守工程职业道德和规范，履行责任	
L09: 个人和团队：能够在多学科背景下的团队中承担个体、团队成员以及负责人的角色	
L10: 沟通：能够就复杂工程问题与业界同行及社会公众进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令。并具备一定的国际视野，能够在跨文化背景下进行沟通和交流	●
LO111：具有基本的成本管理意识，在设计针对复杂物联网工程问题的解决方案时，能够对经济与成本因素加以必要的考量。	
L12: 终身学习：具有自主学习和终身学习的意识，有不断学习和适应发展的能力	

备注：LO=learning outcomes（学习成果）

五、课程目标/课程预期学习成果

学生通过本课程的学习所要达到的业务目标，包括知识目标、能力目标和观念的转变：

- 了解计算机网络和网络安全的基本理论知识；
- 掌握网络安全实验环境的搭建方法；
- 掌握隐写技术，密码学；
- 掌握渗透技术、漏洞挖掘技术；
- 掌握取证技术；

序号	课程预期 学习成果	课程目标 （细化的预期学习成果）	教与学 方式	评价方式
1	LO23：能够对复杂工程问题进行分析和求解，并能通过文献研究或实验寻找可替代的解决方案。	了解相关网络安全理论知识内容，并能对相关 CTF 的比赛有所了解	课堂讲授	实验报告
2	LO52：能够针对复杂物联网工程问题，选择恰当的虚拟仿真工具或方法，对系统或其解决方案进行必要的模拟与预测，并能够理解仿真模拟系统与真实系统之间的差异。	掌握网络环境的搭建，并能对隐写技术，密码学，渗透技术，漏洞挖掘技术，取证技术有所认识和了解	实验操作	实验报告
3	L10: 沟通：能够就复杂工程问题与业界同行及社会公众进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令。并具备一定的国际视野，能够在跨文化背景下进行沟通和交流	了解最新的网络安全技术，并能对国际上发生的各类网络安全事件，网络安全威胁有所了解，具有一定的职业道德和操守	课堂讲授	实验报告 分析报告

六、课程内容

第1单元 网络安全概述

讲解一些基础的网络安全理论知识，并能对基本的网络安全环境搭建有所认识，对VM虚拟机使用，各类软件使用有所认识，对Windows，Linux基本操作有所认识和掌握。

重点：Windows加固，Linux加固；

理论课时数：2

实践课时数：8

第2单元 CTF杂项类型

主要介绍CTF大赛的基本情况，并对杂项类型中隐写技术，密码学和编码，CTF取证技术等内容进行详细介绍，并以实践的方式进行的相关内容操作。

重点：隐写技术

理论课时数：2

实践课时数：2

第3单元 渗透技术

理解WEB渗透测试的基本定义，OWASP标准，渗透基本步骤等，主要讲解相关WEB渗透技术，SQL注入技术，一句话木马技术等内容，要求学生掌握WEB相关内容的技术。

重点：SQL注入，一句话木马

理论课时数：2

实践课时数：8

第4单元 CTF攻防综合技术

使用CTF靶机，实现对于相关技术的综合应用，并能独立分析问题，解决问题，对于攻防过程中遇到的各类问题进行解决。

重点：攻防，夺旗

理论课时数：2

实践课时数：6

七、课内实验名称及基本要求

列出课程实验的名称、学时数、实验类型（演示型、验证型、设计型、综合型）及每个实验的内容简述。

实验序号	实验名称	主要内容	实验时数	实验类型	备注
1	网络安全基本加固	搭建相关实验环境，学会进行windows 和 linux 系统加固	8	综合型	VM虚拟机 Windows操作系统
2	CTF 杂项实验	实现各类杂项技术的操作，包括隐写技术，密码学技术，取证等	2	综合型	VM虚拟机 Windows操作系统
3	渗透实验	实现各类渗透技术的操作，SQL注入，一句话木马等	8	综合型	VM虚拟机 Windows操作系统
4	综合攻防实验	利用靶机实现攻防操作，并实现夺旗	6	综合型	VM虚拟机 Windows操作系统，靶机

八、评价方式与成绩

总评构成（1+X）	评价方式	占比
X1	期末测试	40%
X2	技术文档整理	20%
X3	课程分析报告	20%
X4	实验报告	20%

撰写人：王磊　　系主任审核签名：王磊　　审核时间：2023 年 6 月