【信息安全】

【Information Safety】

一、基本信息

课程代码：【2050132】
课程学分：【3】
面向专业：【网络工程】
课程性质：【选修课】
开课院系：【网络工程系】
使用教材：
教材【网络安全实践教程，王磊，铁道出版社，2018.10】
参考书目【网络信息安全，曾凡平，机械工业出版社，2017.2】
【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：【https://mooc1.chaoxing.com/course/204731062.html】
先修课程：【计算机网络原理 2050064】

二、课程简介

本课程主要介绍和网络安全有关的知识内容，包括计算机网络概述，网络安全概述，操作系统安全，计算机病毒防护，数据加密技术，数据还原技术，防火墙技术，应用服务安全，黑客防范技术，远程控制技术，WEB 渗透技术等内容，通过学习可以使学生对网络环境中存在的各类安全问题都能了解并掌握，为学生提高网络安全意识，并为后续的课程学习提供基础。

三、选课建议

本课程是适用于物联网工程、网络工程专业选修课，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

网络工程专业毕业要求	关联
L01：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网络工程问题	●
L02：问题分析：能够应用数学、自然科学和工程科学的基本原理，识别、表达、并通过文献研究分析复杂网络工程问题，以获得有效结论	
L031：能够针对复杂网络应用需求，通过有效的需求调查与研究、技术分析与设计、流程设计、设备与产品选型，规划与设计满足特定需求的网络系统解决方案，并具有对解决方案进行部署与实施、开发与实现、测试与验证的能力。	
L032：能够认识网络系统及其工程实践对于经济与政治、社会与文化、安全与法律、健康与伦理、环境与可持续发展等的影响，并能够将相关影响作为网络工程需求的组成部分，在解决方案的设计与实施环节中予以综合考虑。	●
L04：研究：能够基于科学原理并采用科学方法对复杂网络工程问题进行研究，包括设计实验、分析与解释数据、并通过信息综合得到有效的结论	

L05：使用现代工具：能够针对复杂网络工程问题，开发、选择与使用恰当的技术、资源、现代工程工具和信息技术工具，包括对复杂工程问题的预测与模拟，并能够理解其局限性	●
L06：工程与社会：能够基于网络工程相关背景知识进行合理分析，评价网络工程实践和复杂网络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网络工程问题的工程实践对环境、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，能够在网络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	
L010：沟通：能够就复杂网络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	●
L011：项目管理：理解并掌握工程管理原理与经济决策方法，并能在多学科环境中应用	
L012：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，操作系统安全加固，计算机病毒防护；
- 掌握 WBE 渗透的基本操作能力，了解基本定义，步骤，工具使用；
- 初步掌握数据加密、恢复、防火墙技术；
- 初步掌握远程控制和黑客防范技术；

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	LO15 能够将网络互联、信息安全、网络测试、网络编程、网络规划与设计等网络工程专业知识，用于复杂网络系统的规划、设计、部署、开发、测试、运维过程中的问题识别与技术分析。	掌握计算机网络原理的相关概念，包括基本定义，层次结构，标准等内容	课堂教学	
2	LO32 能够认识网络系统及其工程实践对于经济与政治、社会与文化、安全与法律、健康与伦理、环境与可持续发展等的影响，并能够将相关影响作为网络工程需求的组成部分，在解决方案的设计与实施环节中予以综合考虑。	掌握网络安全的相关内容，包括网络安全威胁，网络安全关键技术，网络安全法律法规等内容	课堂教学	
3	LO51 能够选择和利用基本的信息技术工具和网络工程工具，结合其他适当的技术与资源，进行复杂网络系统中典型工程问题的预测与分析。	掌握 Windows 操作系统优化的情况下，利用所学习的 Linux 相关知识和 VM 虚拟机工具对 Linux 操作系统进行优化处理，做到提高 Linux 操作系统的安全级别的目的，最终结果以录制屏幕和提交报告为依据	课堂教学	实验报告

4	LO63 能够基于网络工程专业知识，结合“互联网+”相关的应用背景，分析与评价网络系统解决方案或网络工程实践对于社会、健康、安全、法律以及文化的可能影响，并理解组织与个体应承担的责任。	掌握计算机病毒的基本定义后，利用互联网搜索引擎对计算机病毒的各类中毒现象和重大的病毒事件进行梳理，做到能对中毒现象能有较敏感的感知能力	课堂教学	实验报告
5	LO102 能够依照相关的工程标准或行业规范，进行网络工程相关技术问题及文档的书面表达与口头交流。	掌握渗透测试的相关内容，包括基本定义，方法，OWASP TOP 10，特别对 SQL 注入内容有所了解。掌握华为防火墙的基本配置内容，包括 WEB 登录，向导管理等内容	课堂教学	实验报告
6	LO103 具备一门外国语言的基本听、说、读、写、译能力，能够阅读、理解网络工程专业和 IT 技术相关领域的外文资料，具备一定的国际视野，对专业领域相关的新技术具有敏感性。	能自行阅读外文文献资料，并能对开源项目的内容有所掌握实现个人能力的提升	课堂教学	

六、课程内容

第1单元计算机网络概述

理解计算机网络的基本定义、分类、体系结构；理解各类网络协议和子网划分的方法；知道网络设备的种类，网络的未来发展趋势；

重点：OSI参考模型和TCP/IP体系结构的区别；IP地址的分类和子网划分；

理论课时数：4

第2单元网络安全概述

理解网络安全基本定义、网络安全威胁、关键技术、发展历程；理解网络安全涉及主要内容；理解网络安全的法律法规；知道网络安全解决方案；

重点：网络安全法律法规；

理论课时数：6

第3单元操作系统安全

理解操作系统基本定义，能熟练使用DOS命令；能进行Windows操作系统的优化；能进行Linux操作系统的优化；

重点：Windows操作系统优化加固；Windows内网渗透；

理论课时数：10

实践课时数：6

第4单元计算机病毒防护

理解计算机病毒的基本定义、特点、分类、危害、中毒现象分析等；理解计算机病毒防范的基本方法；能使用杀毒软件进行病毒查杀；

重点：手工查杀病毒的基本方法；

实践课时数：4

第5单元 应用服务安全实验

理解应用服务器的基本作用，能搭建各类应用服务器，包括IIS、DNS、FTP等；

重点：IIS服务器搭建；

实践课时数：6

第6单元 防火墙技术

介绍防火墙的基本理论知识,并使用华为防火墙进行基础配置,包括基本的华为防火墙配置，WEB方式登录，NAT转换，双机热备等内容；

重点：防火墙双机热备；

理论课时数：12

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	操作系统安全实验	完成 Windows 操作系统的基本加固操作，包括强密码设置，账户审核策略设置，组策略设置，系统陷阱账户设置，系统数据还原，并能完成系统加固实施方案制订	6	设计型	VM虚拟机 Windows 操作系统
2	计算机病毒查杀实验	对计算机病毒的基本原理，中毒现象有所认识，并能手工查杀各类计算机病毒，例如熊猫烧香，并能完成病毒分析报告	4	设计型	病毒样本
3	应用服务安全实验	要求通过实验可以实现对 WEB 服务器，FTP 服务器，邮件服务器的安装配置，提高服务器安全性能，完成应用服务器安全防范解决方案撰写	6	综合型	应用服务器环境

八、评价方式与成绩

总评构成（1+X）	评价方式	占比
1	期末测试	40%
X1	线上学习及课堂汇报	20%
X2	课程分析表	20%
X3	实验报告	20%

撰写人：王磊　　系主任审核签名：王瑞　　审核时间：2023 年 2 月