【网络管理与安全】

【Network Management and Security】

一、基本信息

课程代码：【0050154】
课程学分：【3】
面向专业：【计算机应用技术】
课程性质：【专业领域课程组】
开课院系：【职业技术学院机电系计算机应用技术专业】
使用教材：
教材【网络安全与管理，清华大学出版社 石磊，赵慧然，肖建良2021.9】
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】
先修课程：【计算机网络技术（3）】

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

本课程是适用于计算机相关专业选修课，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

计算机应用专业毕业要求	关联
L011：表达沟通：能领会用户诉求，正确表达自己的观点，具有专业文档的撰写能力。	
L021：自主学习：能根据环境需要确定自己的学习目标，并主动地通过搜集信息、分析信息、讨论、实践、质疑、创造等方法来实现学习目标。	●
L031：工程素养：掌握数学、自然科学知识，具有工程意识，能结合计算机、计算机网络相关专业知识解决复杂工程问题。	
L032：软件开发：系统掌握基于计算机网络应用系统的设计与开发的基本方法和技能，具备网页设计、网站建设与维护能力。	
L033：系统运维：系统地掌握计算机硬件、软件的基本理论、基本知识，具备保障计算机系统运行与维护基本技能。	
L034：网络工程设计与实施：掌握计算机网络系统的规划、设计方法，具备组建企业或校园网基本技能。	
L035：网络安全管理：系统地掌握信息安全的基本原理和防范策略，具备保障计算机网络安全运行基本技能。	●

L036：网络协议分析：系统地掌握计算机网络协议的基本原理、基本规则，能灵活运用工具实时捕捉数据进行分析。	
L041：尽责抗压：遵守纪律、守信守责；具有耐挫折、抗压力的能力。	
L051：协同创新：能与团队保持良好关系，积极参与其中，保持对信息技术发展的好奇心和探索精神，具有创新性解决问题的能力。	
L061：信息应用：能发掘信息的价值，综合运用相关专业知识和技能，解决实际问题。	●
L071：服务关爱：愿意服务他人、服务企业、服务社会；为人热忱，富于爱心，懂得感恩。	
L081：国际视野：具有基本外语表达沟通能力，积极关注发达国家和地区信息技术发展新动向。	●

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	L021 自主学习：能根据环境需要确定自己的学习目标，并主动的通过搜集信息、分析信息、讨论、实践、质疑、创造等方法来实现学习目标。	学生在了解了网络安全的基本定义的情况下，利用互联网搜索引擎对近三年发生的重大网络安全事件进行整理，做到初步形成网络安全意识，并能对各类网络安全防护手段有所了解和掌握，最终形成分析报告	课堂教学	实验报告
2	L035：网络安全管理：系统地掌握信息安全的基本原理和防范策略，具备保障计算机网络安全运行基本技能。	学生在了解了 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
3	L061：信息应用：能发掘信息的价值，综合运用相关专业知识和技能，解决实际问题。	学生在了解了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，做到对熊猫烧香病毒能有主动查杀的能力，最终结果以录屏的方式和	课堂教学	实验报告
		提交报告为依据		

4	L081：国际视野：具有基本外语表达沟通能力，积极关注发达国家和地区信息技术发展新动向。	学生在了解网络渗透安全的基本定义的情况下，通过利用google 搜索引擎查询国外网站中的 OWASP TOP 10 的基本更新情况，并对网络渗透的基本步骤流程都能了解和掌握，做到能使用工具实现对网站的信息搜集，网站弱点探查，密码破解，用户提权等工作，学生可以整理出一套属于自己的渗透流程，并最终以实验报告的方式提交结果	课堂教学	实验报告

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；能使用Cisco Packet Tracer模拟仿真网络环境；

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；能进行Windows自带防火墙设置；能进行VPN 服务器设置；

重点：网络安全法律法规；VPN 服务器搭建；

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

重点：IIS服务器搭建；Windows操作系统优化加固；Windows内网渗透；

理论课时数：6

实践课时数：20

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；能对逻辑炸弹、熊猫烧香等病毒进行手工查杀；

重点：手工查杀病毒的基本方法；

理论课时数：4

实践课时数：4

第5单元WEB渗透测试技术

理解WEB渗透测试的基本定义，OWASP标准，渗透基本步骤等；能使用手工方式渗透数据库为ACCESS的网站；能使用工具对网站进行渗透测试；

重点：手工渗透测试的方法步骤；使用工具对网站进行渗透测试；

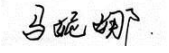
理论课时数：4

七、课内实验名称及基本要求

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	4	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	12	设计型	应用服务器环境
4	远程控制实验	通过实验实现使用灰鸽子软件控制远程服务器的功能，通过控制了解远程控制的基本操作原理	4	设计型	灰鸽子软件

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	60%
X1	平时成绩	40%

撰写人：宋子文　　系主任审核签名： 

审核时间：2022年9月