【网络安全实战】

【Network Security Practice】

一、基本信息

课程代码：【2055053】
课程学分：【2】
面向专业：【计算机科学与技术】专业
课程性质：【系级选修课】
开课院系：【信息技术学院 计算机科学与技术系】
使用教材：主教材：《防火墙和 VPN 技术与实践》，李学昭，人民邮电出版社，出版日期 2022.11。
参考教材：《网络攻防项目实战》，马丽梅，清华大学出版社，出版日期 2022。
先修课程：【计算机网络原理 2050063】

二、课程简介

随着互联网的普及，大量建设的各种网络和信息系统已经成国家、政府和企业的关键基础设施，网络和信息系统已经成为社会和经济发展的强大支柱，同时当前的安全形势也越发严峻，因此对国家和企业的网络安全保障也愈发重要。

本课程描述了网络安全基本概念、防火墙技术、加解密原理和应用、常见网络攻击原理和防范等实践内容，学习本课程后，学生能够掌握搭建小型企业信息安全网络的能力，实现中小企业网络和应用的安全保障。

三、选课建议

本课程是适用于计算机科学与技术专业的系级专业选修课程。要求学生具备一定的网络相关基础知识。

四、课程与培养学生能力的关联性

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工程问题，以获得有效结论	
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	
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	
L05：使用现代工具：能够针对复杂工程问题，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	

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。

拟，并能够理解其局限性	
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	☑
L010：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	
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	☑

五、课程学习目标

以学校培养高层次应用技术型人才的定位目标为导向，本课程理论素养与实践技能培养并重。

通过本课程的教学，使学生了解防火墙，VPN 和攻防技术基础，让学生从攻击中寻求防范方案，由攻击掌握防范方法，在攻击中汲取经验。

在学习防火墙和 VPN 技术的基础上，加强实践技能和动手能力的训练，从而使学生具备设计、部署和运维管理的实践能力。

在课程学习的过程中，掌握对主流 IT 企业官方文档、手册的查阅和使用方法。能够在将来面对新特性新功能，甚至新的开发体系时，能够更快的上手，掌握新的内容。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。

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	L01-3	通过对网络安全技术和架构的学习，未来能够胜任中小企业 IT 架构的网络安全设计，部署和运维管理。	讲课、实验、课堂讨论	实验表现、课程作业
2	L06-2	网络安全是一个集合了多项计算机和 IT 技术的系统性工程，学习本课程后将能够了解网络设备，安全设备和 Linux 操作系统的行业技术标准。	讲授、练习、实践	实验表现、课程作业
3	L09-1	本课程中，同学们将按小组，每位同学分别体验负责不同的项目内容，如：攻击者、网络管理员、系统管理员、安全管理员，通过团队合作，最终完成攻防综合实验。	讲授、练习、实践	实验表现、课程作业

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。

4	LO12-2	掌握对主流 IT 企业官方文档、手册的查阅和使用方法。能够在将来面对新特性新功能，甚至新的开发体系时，能够更快的上手，掌握新的内容。	讲授、练习、课堂讨论	课程作业、在线学习情况

六、课程内容

第 1 单元 网络基础知识

通过本单元学习，使学生理解并掌握数据的定义和传递过程，理解 TCP/IP 协议栈的工作原理，理解常见网络协议的工作原理，了解场景的网络和安全设备及其工作原理。

本章重点：理解 TCP/IP 协议中众多网络协议原理

本章难点：网络安全课程学习需要建立在对网络有一定理解的基础之上，本章的难点就在于需要学生在有限的时间内回顾并实践网络基础知识。

理论课时：0

实践课时：4

第 2 单元 常见网络安全威胁和防范

通过本单元学习，使学生理解企业网络收到的常见网络安全威胁以及常见网络安全威胁的应对方式。

本章重点：常见网络安全威胁的应对方式

本章难点：理解众多网络安全威胁的原理和防范实践。

理论课时：0

实践课时：4

第 3 单元 防火墙安全策略

通过本单元学习，使学生理解并掌握防火墙安全区域的概念，理解防火墙的状态检测和会话机制，描述防火墙在网络中的应用场景，学会基本的防火墙配置。

本章重点：掌握防火墙的基础配置操作

本章难点：理解防火墙应对各种安全威胁的原理和配置。

理论课时：0

实践课时：4

第 4 单元 防火墙网络地址转换技术

通过本单元学习，使学生理解并掌握 NAT 的技术背景，理解 NAT 的分类和技术原理，区分 NAT 技术的应用场景，学会在防护墙配置 NAT。

本章重点：防火墙 NAT 的配置。

本章难点：掌握各种 NAT 技术的配置方法和应用场景。

理论课时：0

实践课时：4

第 5 单元 防火墙双机热备技术

通过本单元学习，使学生理解并掌握 VRRP 协议、VGMP 协议、HRP 协议原理和防火墙双机热备配置，掌握防火墙双机热备基本组网技术。

本章重点：防火墙双机热备技术理解

本章难点：理解防火墙双机热备的组网技术并能够独立配置网络设备配置和防火墙双机热备配置。

理论课时：0

实践课时：4

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。

第 6 单元 防火墙入侵防御

通过本单元学习，使学生理解并掌握入侵防御的种类，理解入侵防御的基本原理，理解如何应用网络反病毒策略。

本章重点：理解常见的入侵手段和其技术原理

本章难点：理解使用防火墙防御常见入侵手段的方法。

理论课时：0

实践课时：4

第 7 单元 加解密技术原理和 VPN 技术应用

通过本单元学习，使学生理解并掌握加解密技术原理和常见加密算法，理解并掌握如 SSL VPN，IPSec VPN 等常见 VPN 技术和配置。

本章重点：理解常见 VPN 技术应用和配置。

本章难点：VPN 技术原理和配置复杂，配置难度高。

理论课时：0

实践课时：4

第 8 单元 攻防演练

通过本单元学习，使学生理解并掌握前面课程讲过的常见网络攻击原理技术和防御手段，通过互相攻防综合演练的方式加深理解。

本章重点：网络攻击和防御实践。

本章难点：需要有一定的 Linux 和网络技术基础，综合性强。

理论课时：0

实践课时：4

注：

1.由于课时紧，内容多，教学进程和内容的深广度将视学生接受程度作适当的调整.

2.教学建议：抓住基本概念、基本原理和基本方法，教法上多举例，重应用。

七、课内实验名称及基本要求（适用于课内实验）

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	防火墙功能实践	1. 防火墙基础配置 2. 安全区域划分 3. 安全策略配置 4. 防火墙基本功能测试	8	验证型	Windows PC 机（8GB 内存） eNSP 软件 Kali Linux 虚拟机一台
2	常见攻击流量防护	1. DDoS 攻击防护配置 2. 内网安全防护配置 3. 网络防病毒配置	8	验证型	Windows PC 机（8GB 内存） eNSP 软件 Kali Linux 虚拟机一台

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。

3	综合实验	Kali Linux和防火墙综合演练	16	综合型	Windows PC 机（8GB 内存） eNSP 软件 Kali Linux 虚拟机一台

以上实验需要写实验报告，其他的实践环节均是配合课堂教学，在课堂上根据进度表进行。

八、评价方式与成绩

总评构成（1+X）	评价方式	占比
1	期末考试	40%
X2	课程作业	30%
X3	实验报告	20%
X4	工作现场评估（出勤情况，课堂表现等）	10%

说明：

总评成绩构成列表中，1 是期末成绩，期终考试内容涵盖本门课程的重难点，采用上机考试形式进行。

其他三项是平时成绩。

X1：实验报告，成绩构成包括各个实验运行结果+实验报告整理情况。

X2：为课程作业，每章节学习均配有相关课程作业，以起到巩固和检测作用，检验本章节学习成果，有针对性的调整教学方案。

X3：工作现场评估，这部分主要根据每次课考勤情况，课堂回答问题情况综合打分。

课程学习建议：要学好本门课程，熟练掌握相关部署和运维管理，自己利用课后时间认真练习是至关重要的，认真实践，课外课内学时比至少达到 3:1。

撰写：陈聪　　系主任审核：戴智明

（2024 年 3 月修订）

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。