【企业网络安全防护】

【Enterprise network security protection】

一、基本信息

课程代码：【2055024】
课程学分：【2】
面向专业：【网络工程】
课程性质：【选修课】
开课院系：【信息技术学院物联网工程系】
使用教材：

教材【网络安全实践教程 铁道出版社 王磊 2018 年 1 月】

参考书目 【信息安全工程师教程（第 2 版）清华大学出版社 蒋建春 2020 年 9 月】
先修课程：【计算机网络原理 2050064（4），信息安全 2050132（3）】
后续课程：【企业生产实践 2059341（2）】

二、课程简介

本课程主要讲解企业网络的相关安全性问题，包括系统安全诊断和加固、网络安全诊断与加固、应用安全诊断与加固、网络安全保障体系建设等内容，通过课程的学习可以帮助学生更好的掌握相关的企业网络的操作技能，学习完课程后可以考取相关证书。

三、选课建议

本课程是适用于物联网工程专业的学科专业选修课程。

四、课程与专业毕业要求的关联性

物联网工程专业毕业要求	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：

- 了解相关的企业网络安全的基本理论知识
- 掌握系统安全诊断的基本操作内容，包括恶意代码，漏洞扫描，系统加固等
- 掌握网络安全诊断的基本方法，包括事件监控，网络安全部署等
- 掌握应用安全的相关内容，包括数据安全，WEB 安全，应用安全漏洞等
- 掌握安全保障体系建设，包括等级保护，基础设施保护，互联网安全等

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	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。	能掌握网络安全的基本理论知识内容	课堂 教学	实验报告
2	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	掌握系统安全诊断，网络安全诊断的相关内容	课堂 教学	实验报告
3	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	掌握数据安全，WEB 安全，等级保护的相关内容	课堂 教学	实验报告

六、课程内容

第1单元 系统安全诊断与加固

本章主要讲解恶意代码防护，漏洞扫描，系统加固等内容，并能对企业网络安全的基本理论知识有所介绍和说明。

重点：漏洞扫描，系统加固；

操作课时数：8

第2单元 网络安全诊断与加固

本章主要讲解网络部署的方法，网络安全事件监控，网络安全传输等方面的内容，对其中的具体操作内容进行详细说明和解释。

重点：网络部署，事件监控

操作课时数：8

第3单元 应用安全诊断与加固

本章主要介绍WEB安全事件分析，数据的安全和恢复，应用安全漏洞扫描等内容，对于其中涉及到企业网络安全漏洞扫描等内容详细进行说明。

重点：数据安全，漏洞扫描

操作课时数：8

第4单元 网络安全保障体系建设

本章主要介绍网络安全等级保护，基础设施安全，互联网安全管理等内容。

重点：等级保护，设施安全

操作课时数：8

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	漏洞扫描实验	进行漏洞扫描操作，并根据漏洞的情况给与相关的修补意见和建议	8	设计型	电脑，虚拟机，漏洞环境
2	网络安全事件监控	进行安全事件的分析，根据分析的结果进行监控，	8	综合型	电脑，虚拟机，
3	数据安全恢复	进行数据安全和恢复操作，能进行 WEB 安全事件分析	8	综合型	电脑，虚拟机，

4	计算机病毒查杀	进行计算机病毒查杀实验内容	8	综合型	电脑，虚拟机，

八、评价方式与成绩

总评构成（1+X）	评价方式	占比
1	证书考证	40%
X1	课程分析报告	20%
X2	实验报告	20%
X3	日常表现	20%

撰写人： 周亚军　　系主任审核签名：王瑞　　审核时间：2022 年 9 月