**信息安全技术**

Information Security Technology

|  |  |  |  |
| --- | --- | --- | --- |
| **课程编号：** | F0303051C | **学 分：** | 2 |
| **开课学院：** | 计算机学院 | **学 时：** | 32 |
| **课程类别：** | 专业课 | **课程性质：** | 限选 |

一、课程的性质和目的

课程性质：本课程是计算机科学与技术等专业留学生的限选课程。

目的：课程介绍了信息安全技术的发展过程和基本概念，包括密码学、电子邮件安全、防火墙、入侵检测系统、网络安全协议、恶意软件等。本课程分析实际网络安全实例，并向学生讲授运用网络安全的基本原理解决网络系统及其应用中安全问题的方法。本课程是一门双语课程，通过课程的学习，让学生能了解信息安全领域中常用的（英文）术语，提高英文阅读能力。

Course Nature and Objective

Course Nature: This course is a specialty course for international students of computer science department.

Objective: This course introduces the development history and basic concepts of information security technology, including cryptography, email security, firewall, intrusion detection system, network security protocol, malware and so on. This course analyzes the practical examples of network security and teaches students how to use the basic principles of network security to solve the security problems of network system and applications. This course is a bilingual course so that students can know commonly-used (English) terms in information security area and improve their reading ability in English during the course.

二、课程教学内容及基本要求

本课程系统介绍网络安全技术的基本理论和方法，课程内容包括密码学、电子邮件安全、防火墙、入侵检测系统、网络安全协议、恶意软件等。通过双语课程学习，使得学生能了解网络安全领域中的（英文）术语，了解网络安全技术及其应用的未来发展趋势。

Course Content and Basic Requirements

This course introduces the basic theories and methods of network security technology systematically, including cryptography, email security, firewall, intrusion detection system, network security protocol, malware and so on. By this bilingual course, students can know commonly-used (English) terms in network security area and understand the future development trend of network security technology and applications.

**（一）课程教学内容及知识模块顺序**

**Course Content and Topic Modules**

1．知识单元一: Introduction（2学时）

Unit 1: Introduction (2 classes)

（1）知识点一：Security Concepts

Topic 1: Security Concepts

（2）知识点二：Security Attacks

Topic 2: Security Attacks

（3）知识点三：Security Mechanisms

Topic 3: Security Mechanisms

（4）知识点四：A Model for Network Security

Topic 4: A Model for Network Security

教学基本要求：

理解网络安全的概念。理解网络安全的历史和安全模型。了解一些商用的网络安全技术产品。

Basic Requirements of Teaching:

Understand the concepts of network security. Understand the history of network security and security model. Know some commercial network security technology products.

2．知识单元二: Cryptography （8学时）

Unit 2: Cryptography (8 classes)

（1）知识点一：Symmetric Encryption and Message Confidentiality

Topic 1: Symmetric Encryption and Message Confidentiality

（2）知识点二：Public-Key Cryptography

Topic 2: Public-Key Cryptography

（3）知识点三：Message Authentication

Topic 3: Message Authentication

教学基本要求：

理解密码学的发展趋势。掌握对称加密和公钥密码系统的原理。理解对称加密与公钥密码系统的不同之处。了解常用的加密算法（如DES,AES,RSA等）。了解消息认证的方法。了解一些常用的安全哈希函数。

Basic Requirements of Teaching:

Understand the development and trend of cryptography. Master the principles of symmetric encryption and public-key cryptography. Understand the difference between symmetric encryption and public-key cryptography. Know some commonly-used cryptography algorithm, such as DES, AES, RSA. Know message authentication methods. Know some commonly- used secure hash function, such as MD5, SHA-1.

3．知识单元三: Email Security （2学时）

Unit 3: Email Security (2 classes)

（1）知识点一：Pretty Good Privacy

Topic 1: Pretty Good Privacy

（2）知识点二：S/MIME

Topic 2: S/MIME

（3）知识点三：DomainKeys Identified Mail

Topic 3: DomainKeys Identified Mail

教学基本要求：

掌握PGP技术在电子邮件中的应用。理解S/MIME的定义。简要了解DKIM技术。

Basic Requirements of Teaching:

Master the Pretty Good Privacy (PGP) technology for email security. Understand the formal definition of S/MIME. Know something about DomainKeys Identified Mail (DKIM).

4．知识单元四: Firewall （2学时）

Unit 4: Firewall (2 classes）

（1）知识点一：Firewall Design Principles

Topic 1: Firewall Design Principles

（2）知识点二：Deployment of Firewall

Topic 2: Deployment of Firewall

（3）知识点三：Common Firewall Products

Topic 3: Common Firewall Products

教学基本要求：

了解防火墙的需求。掌握防火墙设计的基本概念。掌握防火墙部署的方法。了解一些常用的防火墙产品。

Basic Requirements of Teaching:

Know the requirements for firewall. Master basic concepts about firewall design. Master how to deploy firewall in networks. Know some common firewall products.

5．知识单元五: Intrusion Detection System （4学时）

Unit 5: Intrusion Detection System (4 classes)

（1）知识点一：Intruders

Topic 1: Intruders

（2）知识点二：A Model for Intrusion Analysis

Topic 2: A Model for Intrusion Analysis

（3）知识点三：Misuse Detection and Anomaly Detection

Topic 3: Misuse Detection and Anomaly Detection

（4）知识点四：Honey Pot

Topic 4: Honey Pot

（5）知识点五：Snort

Topic 5: Snort

教学基本要求：

了解如何设计入侵检测分析模型。掌握两种基本的分析模型——误用检测和异常检测。了解蜜罐技术。理解如何使用Snort。

Basic Requirements of Teaching:

Know how to design intrusion analysis model. Master two basic analysis schemes: misuse detection and anomaly detection. Know something about Honey Pot. Understand how to use Snort.

6．知识单元六: Web Security （2学时）

Unit 6: Web Security (2 classes)

（1）知识点一：Web Security Requirements

Topic 1: Web Security Requirements

（2）知识点二：Secure Socket Lay and Transport Layer Security

Topic 2: Secure Socket Lay and Transport Layer Security

（3）知识点三：HTTPS

Topic 3: HTTPS

（4）知识点四：SSH

Topic 4: SSH

教学基本要求：

理解Web安全的要求。掌握SSL和TLS协议中的握手过程。了解HTTPS原理。了解SSH原理。

Basic Requirements of Teaching:

Understand the requirements for web security. Master the handshaking process of SSL and TLS protocols. Know the principles of HTTPS. Know the principles of SSH.

7．知识单元七: Wireless Network Security （2学时）

Unit 7: Wireless Network Security (2 classes)

（1）知识点一：IEEE 802.11 Wireless LAN

Topic 1: IEEE 802.11 Wireless LAN

（2）知识点二：WLAN Security

Topic 2: WLAN Security

（3）知识点三：WEP and WPA

Topic 3: WEP and WPA

教学基本要求：

了解IEEE 802.11 Wireless LAN标准。了解无线局域网安全的概念。理解WEP和WAP协议。

Basic Requirements of Teaching:

Know IEEE 802.11 Wireless LAN standard. Know WLAN security. Understand WEP and WAP.

8．知识单元八: Malware（2学时）

Unit 8: Malware (2 classes)

（1）知识点一：Malware Overview

Topic 1: Malware Overview

（2）知识点二：Virus

Topic 2: Virus

（3）知识点三：Distributed Denial of Service Attacks

Topic 3: Distributed Denial of Service Attacks

教学基本要求：

了解恶意软件的基本概念。理解病毒的机制和防御手段。了解DDoS的基本概念。

Basic Requirements of Teaching:

Know the basic concepts of Malware. Understand the mechanisms of computer viruses and how to defend virus. Know the basic concepts of distributed denial of service attacks (DDoS).

**（二）课程的重点、难点及解决办法**

重点：网络安全技术的基本概念和原理，密码学，电子邮件安全，防火墙，入侵检测系统，网络安全协议，恶意软件，信息安全领域常用的（英文）术语。

难点：对称密码算法，分布式拒绝服务攻击的防范，防火墙的部署和设置，入侵检测系统Snort。

解决办法：

理论课的教学要充分利用多媒体课件辅助课堂教学，用典型实践案例对学生进行讲解，激发学生的学习兴趣。使学生在了解案例的同时，熟悉并掌握相关技术的发展现状、基本概念等。

课堂上的时候应当进行现场演示，通过理论联系实际的方法，使得学生实际了解信息安全的具体需求，培养学生思考和解决实际问题的能力。

**Key points, difficulties and solutions of the course**

Key points: the basic concepts and principles of network security technology, cryptography, email security, firewall, intrusion detection system, network security protocol, malware, commonly-used (English) terms in information security area.

Difficulties: symmetric encryption algorithm, prevention of DDoS, deployment and configuration of firewall, intrusion detection system Snort.

Solutions:

Theory class should take full use of multimedia courseware in the classroom teaching. Explain to the students with typical practice cases in order to stimulate students' interest in learning. So that students can understand the cases and master current situation of the related technology, basic concepts and so on.

Demonstration should be used during class. By the method of theory with practice, students can understand the specific requirements of information security and also develop their ability in thinking and solving practical problems.

三、实验实践环节及基本要求

**Experimental Practice and Basic Requirements**

1．实验实践环节在本课程中的作用及要求（实验教学大纲单独编写）

实验实践环节是对课程知识的进一步巩固，并锻炼解决实际问题的能力。本课程是实践性很强的课程，学生通过实验才能更好地理解理论知识，将这些理论知识用于解决网络安全的实际问题。

在8学时的实验中，要求学生通过实验，熟悉网络安全工具，掌握常见的信息安全防护技术，打下扎实的科研与工程实践基础。

The Function and Requirements of Experimental Practice (the experiment syllabus is written separately)

Experimental practice is to further consolidate the curriculum knowledge and also train the ability in solving practical problems. This course is a practical course. Student can better understand the theoretical knowledge through experiments and solve the practical problems of network security with the knowledge.

During the 8 classes of experiments, students should get familiar with network security tools, master the common information security technology, and lay a solid foundation for scientific research and engineering practice.

2．实验项目(具体要求见实验教学大纲)

实验一：Implement and Defense of Common Network Attacks（2学时）

实验二：SSL Encryption（2学时）

实验三：Intrusion Detection System（2学时）

实验四：Wireless Network Security（2学时）

Experimental Projects (specific requirements are referred to the experiment syllabus)

Experiment 1: Implement and Defense of Common Network Attacks (2 classes)

Experiment 2: SSL Encryption (2 classes)

Experiment 3: Intrusion Detection System (2 classes)

Experiment 4: Wireless Network Security (2 classes)

四、本课程与其它课程的联系与分工

先修课程：计算机网络或计算机通信相关的课程。

Relations and Role Difference between This Course and Others

Prerequisites for the course: computer networks or computer communication related courses.

五、对学生能力培养的要求

通过课程学习，使学生在掌握信息安全的基本概念，提高学生对信息安全技术的理解和应用能力。

Students Ability Requirement

Through the course, students can master the basic concepts of information security and improve their understanding of information security technology as well as the application ability.

六、课程学时分配

总学时32，其中讲课24学时，实验8学时。课程主要内容和学时分配见课程学时分配表。

**课程学时分配表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 教学环节  时数  课程内容 | 讲课 | 上机 | 实验 | 课外 | 小计 |
| Introduction | 2 |  | 2 |  | 4 |
| Cryptography | 8 |  | 2 |  | 10 |
| Email Security | 2 |  |  |  | 2 |
| Firewall | 2 |  |  |  | 2 |
| Intrusion Detection System | 4 |  | 2 |  | 6 |
| Web Security | 2 |  |  |  | 2 |
| Wireless Network Security | 2 |  | 2 |  | 4 |
| Malware | 2 |  |  |  | 2 |
| 总计 | 24 |  | 8 |  | 32 |

七、建议教材和教学参考书目

**1．教材**

William Stallings, Network Security Essentials: Applications and Standards (Fourth Edition, 影印版)，北京：清华大学出版社，2010

**2．主要参考书**

[1] William Stallings, 网络安全基础：应用与标准（第四版）. 白国强等译，北京：清华大学出版社, 2011

[2] William Stallings. 密码编码学与网络安全：原理与实践（第5版）.王张宜等译.北京：电子工业出版社,2011

[3] 陈伟，李频．网络安全原理与实践．北京：清华大学出版社，2014年

[4] Joshi Bagchi，etc. Network Security．Elsevier Inc., 2008.

八、课程考核

本课程采用开卷考试方式，平时成绩占总评的30%，期末成绩占总评的70%。平时成绩从作业、上课出勤率、实验等方面进行考核。

执笔人：朱枫 审核人： 陈伟 教学院长：张伟