## 《网络安全技术》教学大纲

|  |  |  |  |
| --- | --- | --- | --- |
| 课程性质 | 专业必修课 | 课程代码 |  |
| 总学时数 | 51，其中理论：34实践：17 | 学 分 数 | 3 |
| 适用专业 |  | 先修课程 | 计算机网络、密码学 |
| 课程负责人 |  | 主讲教师 |  |

一、课程教学目标

本课程主要介绍计算机网络安全概述、数据加密技术及应用、PKI/PMI技术及应用、身份认证技术、TCP/IP体系协议安全、防火墙技术及应用和VPN技术及应用等知识。通过该课程学习，学生应当：

1.了解网络安全技术目前的学术、研究和应用等方面的状况，理解网络安全技术中的主要概念和相关基础理论。

2.力求使学生能够掌握常见的网络安全技术工具的使用，同时具有一定的解决网络安全问题的实际能力，为在今后的专业学习中和从事网络安全执法工作打好坚实的理论基础和锻炼出一定的实际动手能力。

3.关注网络安全相关理论和热点问题，能够主动发现问题，分析问题，并以创新的方法解决问题，为今后的发展、创新打下良好的基础。

二、课程主要教学内容与学时分配

（一）理论教学

本课程理论教学共34课时，主要分为以下模块：模块一，网络安全基础；模块二，网络安全技术。具体安排如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 教学模块 | 教学单元及知识点 | 教学重点与难点 | 课时数 |
| 模块一  网络安全基础 | 计算机网络安全概述：计算机网络安全问题、网络安全的概念，网络安全威胁的类型、安全安全策略和安全等级、常用的网络安全管理技术。 | 网络安全威胁的类型  安全策略和安全等级 | 4 |
| 数据加密技术及应用：数据加密概述、对称密码学、非对称密码学、消息认证与hash函数、数字签名。 | DES、RSA、消息认证和数字签名 | 4 |
| 模块二  网络安全技术 | PKI/PMI技术及应用：公钥基础设施PKI技术，PKI/PMI的基本概念、组成和功能，认证机构，证书及管理 | PKI/PMI的概念、组成和功能；证书及管理 | 4 |
| 身份认证技术：身份认证的概念，基于密码的身份认证，基于地址的身份认证，基于生物特征的身份认证以及相关的身份认证协议。 | 身份认证概念、类型  身份认证协议 | 6 |
| TCP／IP体系的协议安全：TCP/IP体系以及相关协议安全，ARP安全，DHCP安全，TCP 安全，DNS安全。 | ARP欺骗、DHCP的安全、TCP的安全、DNS的安全 | 8 |
| 防火墙技术及应用：防火墙的概念和应用，防火墙的类型，个人防火墙技术。 | 防火墙的概念、基本类型 | 4 |
| VPN技术及应用：VPN技术概述、隧道技术、VPN实现技术。 | VPN的基本类型、应用及实现技术 | 4 |
| 总时数 | |  | 34 |

（二）实践教学

本课程实践教学共17课时，主要分为以下实验：实验一，密码应用；实验二，PKI/ PMI原理与应用；实验三，身份认证；实验四，ARP欺骗攻击；实验五，防火墙的配置与应用；实验六，VPN技术。具体安排如下：

**实验一：密码应用，3课时**

实验目的：1.学会使用常用软件对Word进行电子签名；2.学会利用PGP工具实现安全通信；3.理解安全通信的实现过程。

实验内容：1.安装iSignature按钮， Word签名实验；2.PGP安全通信。

实验条件：每组二人，Windows网络环境，交换网络环境。

教学组织：每组二人，每组设小组长一名负责总结汇报。

相关要求：熟悉iSignature等工具的使用方法，完成相关实验报告。

**实验二：PKI/ PMI原理与应用，3课时**

实验目的：1.加深理解PKI体系；2.掌握PMI的使用过程 ；3.理解PMI和PKI的关系。

实验内容：1.使用PKI工具实现安全通信；2.PMI应用（生成公钥证书、证书申请、请求管理、证书管理、属性管理）。

实验条件：每组三人，Windows网络环境，交换网络环境。

教学组织：每组三人，每组设小组长一名负责总结汇报。

相关要求：1.熟悉PKI工具使用方法；2.掌握PMI的基本概念；3.完成相关实验报告。

**实验三：身份认证，3课时**

实验目的：1.了解用户名密码及数字证书认证方式及其优缺点；2.学习Kerberos身份认证过程。

实验内容：1.静态口令身份认证、数字证书身份认证；2.Kerberos安全认证协议。

实验条件：每组6人 ，Windows网络环境，交换网络环境。

教学组织：每组三人，每组设小组长一名负责总结汇报。

相关要求：完成相关实验报告。

**实验四：ARP欺骗攻击，2课时**

实验目的：1.掌握ARP欺骗原理及过程；2.学会如何防范ARP欺骗攻击。

实验内容：1.ARP欺骗（正常通信、ARP攻击、单向欺骗、完全欺骗）；2.防范ARP欺骗（清空ARP缓存表、IP/MAC地址绑定、ARP监听）。

实验条件：Windows LINUX ，交换网络环境。

教学组织：每组三人，每组设小组长一名负责总结汇报。

相关要求：1.本实验使用交换网络结构，组一、二和三间通过交换模块连接；2.主机C要监听主机A和主机E间的通信数据，主机D要监听主机B与主机F间的通信数据。

**实验五：防火墙的配置与应用，3课时**

实验目的：1.了解防火墙的含义及作用；2.学习防火墙的基本配置方法。

实验内容：1.Windows防火墙配置；2.Linux防火墙配置；3.企业级防火墙配置。

实验条件：交换网络环境。

教学组织：每组2-3人，每组设小组长一名负责总结汇报。

相关要求：完成相关实验报告。

**实验六：VPN技术，3课时**

实验目的：1.理解VPN工作原理；2.利用Windows系统自带工具搭建基于PPTP的VPN；3.建立 SSL VPN安全隧道。

实验内容：1.利用PPTP构建企业VPN；2.利用SSL构建企业VPN。

实验条件：Windows网络环境，交换网络环境。

教学组织：每组3人，每组设小组长一名负责总结汇报。

相关要求：1.掌握VPN的原理、隧道技术；2.完成相关实验报告。

三、教学方法与策略

课堂导入可通过多媒体短片、案例导入、问题导入等方式，改变传统计算机网络课堂教学中单一、乏味的局面，在激发学生学习兴趣的同时，提高学生分析问题，解决问题的能力。

课堂教学可通过案例教学、分组讨论等形式，做到每一教学模块至少安排一次案例讨论，提高学生学习积极性，培养学生合作学习能力及小组团队意识。

课后巩固可通过课后作业形式，做到每一教学模块至少安排一次课后作业，教师及时批改并进行反馈。

四、学生学习成效评估方式

本课程对学生的学习成效评估分为以下三部分：平时表现（10%）+平时作业（15%）+期末考试（75%）。

平时表现：学生出勤率及课堂表现。

平时作业：平时作业是分阶段地布置一些作业，然后教师对学生的完成情况做出相应的评价，然后适时地调整教学计划。

期末考试：采用闭卷书面考试的形式。

五、适用教材

王群，李馥娟．网络安全技术．清华大学出版社．202011

六、参考资料

[1] 王群．计算机网络安全技术．清华大学出版社．

七、思政

1. 培养学生民族认同感，树立远大职业理想。梳理国产操作系统的发展历史与现状，包括华为、中兴等国产企业在全球市场的崛起，在操作系统领域的新架构，向学生展示中国的信息技术领域成就，增强使命感与荣誉感；通过华为孟晚舟事件、美国的芯片垄断—引出：民族认同感。党的十八届五中全会通过的“十三五”规划《建议》，明确提出实施网络强国战略以及与之密切相关的“互联网+”行动计划。国家正着力实现关键技术自主可控，为维护国家安全、网络安全提供技术保障。中国信息化需求巨大，但在一些关键技术领域如操作系统、芯片技术、CPU 技术等方面，还难以做到自主可控，对国家安全造成威胁。引导学生明确：建设网络强国，不仅仅是靠网络技术，还要有软件技术等其他各类技术的支撑。引导学生作为软件技术专业的一员，应更加明晰专业人才的培养目标，更加明确专业领域内工作岗位和工作内容的社会价值，自觉树立远大职业理想，将职业生涯、职业发展脉络与国家发展的历史进程融合起来。

2. 通过专业知识的学习，引导学生深刻理解与认识所学软件开发知识对于国家信息产业发展、智慧城市建设、大数据智能信息处理等各方面的重要意义，使学生在学习过程中逐渐树立专业荣誉感；

3.培养学生精益求精、工匠精神。告诉学生在学好软件技术之后，走上工作岗位会成为程序员、软件系统运维人员、软件测试员、售前售后服务人员等。在这些职位岗位上，要发挥工匠精神，精益求精地将程序开发、系统运维、程序测试、需求分析及技术问题处理等工作内容完成好，保证软件系统运行时正确、稳定，保证客户的需求被精确采集和纳入软件开发计划，保证软件运行时遇到问题能被及时解决。引导学生在学习时，将知识夯实、精技强能，方能在今后工作中本领过硬，不出纰漏，工作成果令用户满意。引导学生认识到，作为职业人，其专注、敬业、责任担当对完成好本职工作，进而促进软件行业整体的高水平、优质化发展具有重要意义。

4.培养学生团结协作，合作共赢的精神。通过实践项目、竞赛等，告诉学生今天的社会无论什么行业想要做出一番成就，靠一个人打拼已经不现实了。所谓人多力量大，三个臭皮匠顶个诸葛亮... ... 强调团队成员之间的资源共享、协同合作精神，团队成员在一个项目中要各司其职，每个人发挥自己的特长完成分配的任务，最终才能高质量、有效率地完成项目，从而形成更强大而持久的生产力和创造力。