**《 ★渗透测试 》 课程标准**

一、课程基本信息

|  |  |
| --- | --- |
| **课程名称:★渗透测试** | |
| **课程编码:05051044** | **课程类别:专业必修课** |
| **学分:5** | **学时：90** |
| **适用专业:计算机信息管理** | **开课单位:智能信息工程学院** |
| **先修课程:★Windows服务器配置与管理(05041009),Linux服务器配置与管理(05041004),★信息安全产品配置与应用(05051043)** | **后续课程:★信息安全管理(05031134)** |

二、课程概述

（一）课程定位

本课程是计算机信息管理专业的一门专业必修课程。渗透测试是一种通过模拟恶意黑客的攻击行为，来评估计算机网络系统安全的方法。通过学习该课程,加深学生对信息安全原理的理解，初步掌握网络攻防的主要技术环节和操作方法，并在此基础上强化学生的实践意识，提高其技术实践能力与技术应用能力。
本课程的前驱课程有：《计算机应用基础》、《计算机网络技术》、《Windows服务器配置与管理》、《Linux服务器配置与管理》、《信息安全产品配置与应用》等，后继课程有：《信息安全管理》、《毕业设计》、《顶岗实习》等。本课程90课时（50理论+40实践），因课程实践性较强，在教学过程中，建议采用理实一体化。

（二）课程基本理念

本课程秉承如下的基本理念：
1、坚持以服务为宗旨，以促进就业为导向的专业建设方针。
计算机信息管理专业主要面向IT行业及信息化产业的企事业单位，培养思想政治坚定、德技并修，适应新时期国家和地方信息化建设需要，具有良好的道德文化素质、专业素质、心理素质、身体素质等，掌握计算机信息管理的基本理论知识与职业技能，能够完成企业信息系统的规划和建设，数据库应用程序开发与维护、电子商务实施等工作，具备网络安全运维与管控、信息安全设备调试以及企业信息的安全防护，面向国家各级管理部门、工商企业、金融机构、科研单位等部门从事计算机与信息管理和服务的德智体美劳全面发展的高素质技术技能人才。本课程是为培养上述专业学生的网络安全运维与管控能力而开设的一门课程，将使学生掌握相关岗位所需要的知识和技能，为学生将来的就业服务社会打下相关知识和技能的基础。
2、坚持“校企合作”共建专业的办学模式。
在进行课程建设的过程中，坚持校企合作，是职业院校提升办学内涵的重要抓手，也是我们始终坚持的原则，在具体实施过程中，我们通过以下几点来实现在课程建设中有机的融合校企合作的理念。
（1）以职业体验为基点。通过校企合作，让学生走进工作现场，切实感受相关岗位的工作内容，认识到该门课程在工作过程中的作用，形成初步的职业体验。
（2）以知识应用和拓展为过程。校企合作的课程注重岗位实践与知识、技能的有机融合，让学生既掌握相关岗位所需的知识、技能，又为今后的进一步发展打下基础。
（3）以职业倾向为导向。学习职业技能课程的知识和技能，深入企业生产第一线，学生能够了解基本的职业概况，体验职业快乐，从中找到自己的兴趣所在，从而形成职业倾向，奠基未来发展。
3、坚持“工学结合”的高职人才培养模式。
建立工学结合课程包括如下的内容：
（1）明确促进综合职业能力发展的培养目标；
（2）构建学习领域的课程；
（3）通过职业资格研究确保职业分析的质量；
（4）通过分析典型工作任务确定课程门类；
（5）按照工作过程系统化得原则确立课程结构；
（6）按照职业成长的逻辑规律排列课程序列；
（7）采用便于学生自主学习的课业方式组织课程内容；
（8）按照行动向导原则实施教学；
（9）建设以专业教室和工学整合式学习岗位为代表的教学环境；
（10）建立以过程控制为基本特征的质量控制与评价体系。
4、坚持“以学为本 ”的教育理念和“以学生为主体”的教学理念。
以学为本是以人为本思想在高职教育领域中的体现，是育人的核心理念。在课程建设中体现以学为本，就是要从如下3点入手：
（1） 了解我们的学生，热爱我们的学生。
（2） 因材施教。
（3） 以学生为主体组织教学内容，开展教学。
5、坚持职业能力培养为主线，加强实践能力培养。
学生职业能力培养是高职教育的主要任务，而课程教学又是培养学生职业能力的关键。在“以职业能力分析为基础，以工作过程为导向”的课程建设理念指导下，构造“以工作过程为能力主线，以职业能力为课程核心，以职业标准为课程内容，以教学模块为课程结构，以最新技术为课程视野，以双师团队为课程保障”的课程建设方案。该课程方案坚持职业能力培养为主线，加强实践能力培养。
6、加强素质教育，强化职业道德。
高职院校以培养高素质的技能人才为主要目标，高职学生的职业素质是指高职学生今后能够胜任社会职业所必须具备各种素质的总称，它不仅包括思想道德素质、专业技能素质还包括人际沟通、自我管理、团队协作、创新创业等素质。
课程建设中既要考虑提升学生综合素质，又要结合学生岗位工作过程为学生的职业能力养成提供支撑。使学生具备基本的职业素养和职业通用的人际沟通能力，主要包括口语表达能力、实用写作能力、沟通交际能力等。进一步教育学生学会做人、学会做一个优秀的职业人，真正实现高职教育“能说会做有修养”的培养目标。

（三）课程设计思路

首先依据专业人才培养方案中关于人才培养目标的阐述，明确课程目标；其次，结合职业教育课程观、教学观、能力观，基于本专业相关岗位的工作过程，以项目化教学来组织课程内容，在课程内容的选择与排序中，以本专业典型岗位对知识和技能的不同要求、典型任务为载体，将课程内容划分为互相联系的学习情景；第三，通过对各学习情景中学习目标、主要内容、授课方式、师生要求等各项内容的描述，来规范课程所要求的内容；第四，通过对课程内容的选取和组合，以一个完整的项目为载体，完成课程的实施；最后，通过对项目实施过程中各个环节的考察和评价，来完成对课程的评鉴与考核。
本课程在设计上本着懂方法，重应用的总体思路，突出体现职业教育的技能型、应用性特色，着重培养学生的实践应用技能，力求达到理论方法够用，技术技能过硬的目的。

三、课程目标

（一）总目标

本课程主要帮助学生掌握网络安全的基本实用技术，巩固和扩大信息安全理论课程的基础理论知识，对信息安全体系结构和各种安全服务及安全机制有更深入的认识和掌握。

（二）具体目标

|  |  |
| --- | --- |
| **序号** | **知识目标** |
| **K1** | 理解计算机网络攻击的主要原理 |
| **K2** | 掌握渗透测试的定义和分类 |
| **K3** | 掌握渗透测试的流程 |
| **K4** | 掌握SQL注入漏洞的利用与防御 |
| **K5** | 掌握Web渗透测试基础 |
| **K6** | 掌握跨站脚本漏洞原理与用法 |
| **K7** | 掌握常见Web漏洞原理与用法 |
| **K8** | 掌握端口扫描的原理与用法 |
| **K9** | 理解操作系统典型漏洞原理 |

|  |  |
| --- | --- |
| **序号** | **技能目标** |
| **S1** | 掌握账号安全管理 |
| **S2** | 掌握网络嗅探操作方法 |
| **S3** | 掌握操纵系统典型漏洞利用。 |
| **S4** | 掌握缓冲区溢出的原理和防范 |
| **S5** | 掌握木马攻击的原理和防范 |
| **S6** | 掌握sqlmap工具使用 |
| **S7** | 掌握nmap端口扫描操作 |

|  |  |
| --- | --- |
| **序号** | **态度目标** |
| **A1** | 能理论结合实践，培养良好的动手能力 |
| **A2** | 具备爱岗敬业、吃苦耐劳的良好职业道德 |
| **A3** | 具有团队意识，能协作完成任务 |
| **A4** | 具有自主学习能力和自我提高能力 |
| **A5** | 具有分析问题和解决问题的能力 |

四、课程内容

|  |  |  |
| --- | --- | --- |
| **序号** | **模块（或子模块）名称** | **学时** |
| **1** | 渗透测试概述 | **4** |
| **2** | Web渗透测试基础 | **8** |
| **3** | SQL注入漏洞利用与防御 | **14** |
| **4** | 跨站脚本漏洞利用与防御 | **14** |
| **5** | 常见Web漏洞利用与防御 | **14** |
| **6** | 常见的端口扫描与利用 | **12** |
| **7** | 操作系统典型漏洞利用 | **12** |
| **8** | 典型案例分析 | **12** |
| **合 计** | | **90** |

1. 学习任务
2. 设计思路

本课程的教学以高等职业教育培养目标为依据，遵循“结合理论联系实际，应知、应会”的原则，以拓展学生专业知识覆盖面为重点； 注重培养学生的专业思维能力。以工作过程为导向采用项目教学法或翻转课堂教学法进行教学，通过案例演示，提出问题，给出知识点，讲解案例应用背景，给学生一个切入点，建立感性认识，明确本次课的教学目标。设计思路以点带面，引导学生自主学习，找到解决问题的方法和操作技能，培养学生的自主学习意识和学习方法。为了使学生能学以致用、举一反三、触类旁通，每次教学结束时及时布置相关的课后练习，使学生在课后进一步复习巩固，从而带动整个知识面的学习。

(二)学习任务

注：本表格中的“覆盖目标”只需填写在第三部分所确定的学习目标的编号。

|  |  |  |  |
| --- | --- | --- | --- |
| **任务**  **序号** | **任务** | **子任务** | **覆盖**  **目标** |
| T1 | **渗透测试概述** | **T1-1 | 网络安全概述**  **T1-2 | 渗透测试的定义和分类**  **T1-3 | 渗透测试的流程** | K1,S1,A1,A2,A3,A4,A5 |
| T2 | **Web渗透测试基础** | **T2-1 | Web渗透测试常用术语**  **T2-2 | 搭建Web服务器环境**  **T2-3 | 不同Web/DB组合类型的渗透测试思路**  **T2-4 | Web渗透测试常用工具介绍**  **T2-5 | WebShell的常用工具介绍** | K2,S1,S4,A1,A2,A3,A4,A5 |
| T3 | **SQL注入漏洞利用与防御** | **T3-1 | 发展历史**  **T3-2 | 形成原因**  **T3-3 | 利用方式**  **T3-4 | SQL注入的危害**  **T3-5 | 防御基础及实例分析** | K3,K4,S1,S2,S3,A1,A2,A3,A4,A5 |
| T4 | **跨站脚本漏洞利用与防御** | **T4-1 | XSS漏洞的危害**  **T4-2 | 防御基础** | K5,S3,S4,A1,A2,A3,A4,A5 |
| T5 | **常见Web漏洞利用与防御** | **T5-1 | 遍历目录**  **T5-2 | 弱口令**  **T5-3 | 解析漏洞**  **T5-4 | 上传漏洞**  **T5-5 | 系统命令执行漏洞** | K6,S1,S2,S4,A1,A2,A3,A4,A5 |
| T6 | **常见的端口扫描与利用** | **T6-1 | 端口的基本知识**  **T6-2 | 几种常见的端口检测** | K7,S1,S4,S5,A1,A2,A3,A4,A5 |
| T7 | **操作系统典型漏洞利用** | **T7-1 | 操作系统漏洞概述**  **T7-2 | MS08-067**  **T7-3 | 漏洞的介绍及测试**  **T7-4 | Linux操作系统安全漏洞** | K8,S1,S3,S6,A1,A2,A3,A4,A5 |
| T8 | **典型案例分析** | **T8-1 | ECShop渗透测试案例**  **T8-2 | DedeCMS渗透测试案例**  **T8-3 | 利用已知漏洞渗透案例**  **T8-4 | Wi-Fi渗透案例** | K9,S1,S3,S7,A1,A2,A3,A4,A5 |
|
|
|

1. 实施建议

(一)组织实施建议

以工作过程为导向采用项目教学法或翻转课堂教学法进行教学，让学生能在项目中学习，激发学生的学习兴趣，并有效地调动学生的学习积极性。具体方法如下：
1、可以将“教、学、做”融为一体。
①案例引入，提出问题。
通过案例演示，提出问题，给出知识点，讲解案例应用背景，给学生一个切入点，建立感性认识。目的是激发学生的学习兴趣、让学生感到学有所用，从而明确本次课的教学目标。
②学生自主学习，尝试解决问题。
引导学生自主学习，找到解决问题的方法和操作技能，培养学生的自主学习意识和学习方法。学生在学习和尝试解决问题过程中，发现问题，提出问题，在问题的引导下学习相关的知识和操作技能。
③归纳总结，引申提高。
在每次课结束前，引导学生进行归纳总结。对本次课的实际意义、重点、难点、容易出错处等及时进行总结。并针对案例的不足之处，进行引申和提高。注意在这个阶段，强调的是“引导”学生，而不是老师讲解。
④举一反三、学以致用。
为了使学生能学以致用、举一反三、触类旁通，每次教学结束时及时布置相关的课后练习，使学生在课后进一步复习巩固，并且将课后作业纳入形成性考核的内容之一。同时给出下一次课的学习内容，提示学生预习。
2、充分利用现代化教学手段，提高教学效果
教学中采用电子演示文稿、大屏幕多媒体联机演示、网络教学等各种先进的教学手段，使课堂教学生动活泼、引人入胜，提高了教学效果，同时提高了教学效率。
3、构建学习资源平台
教师可将该课程的课程标准、教案、习题、实验指导、参考资料、教学录像等内容全部上网，并向学生免费开放，通过网络化的教学方式（网络课件、网上答疑、网上提交作业、视频点播），学生可以在课外自主学习，以强化、巩固和拓展教学内容。

(二)教材编写建议

1、教材编写要以能力训练为主线编写，注重教材与实际的衔接。
2、教材应体现职业教育特点和现代意识，关注计算机发展、网络更新。
3、教材要增大案例比例，以案例教学增强学生对知识点的理解和对技能的掌握。
4、教材应附和职业技术类院校学生参差不齐的发展特点，适应学生的认知水平，密切联系学生的经验世界和想象世界，有助于激发学生的学习兴趣和创新精神。
5、教材案例要具有典范性，风格丰富多样，难易适度，适合学生学习。

(三)实验实训设备配置建议

本课程要求在理论实践一体化教室（多媒体教室）完成，以实现“教、学、做”合一，硬件配置符合最新操作系统的建议配置，同时实验用计算机的操作系统尽可能和微软同步。实验计算机还要求安装多媒体教学软件，方便下发教学任务和收集学生课堂实践任务。

(四)课程资源开发与利用建议

教师可以利用校内共享课程资源平台，开发《渗透测试》课程的共享资源，向学生提供优质学习资源。

(五)教师要求

必须具备双师素质，有一定的开发经验，对代码规范性有较好的理解。
在教学组织能力方面，本课程的主讲教师具备基本的设计能力，即根据本课程标准制订详细的课程授课计划，对每一堂课的教学过程精心设计，做出详细、具体的安排；还应该具备较强的施教能力，即掌握扎实的教学基本功并能够因材施教，在教学过程中还应具备一定的课堂控制能力和应变能力。

(六)教学管理

教学管理是在主管院长的领导下，实行学院、分院（系）两级负责，学院是教学 管理的主体力量，主要通过以下形式进行：
1.建立教学管理组织协调系统，专业教研室配合教务处、各分院（系）对日常课堂教学及教学建设工作进行管理和监控，及时解决教学中出现的问题。
2.学院、分院（系）两级督学系统，聘请有丰富教学经验和教学管理经验的老教师与其他教学管理人员组成校院两级科学小组，实现“督教、督学、督管”。
3.分院（系）同行教师评价系统，由分院（系）进行主讲教师的聘任，教师试讲和 教学效果评价工作。
4.学生信息员系统，聘任学生担任本专业的教学质量监督言息员，及时掌握专业的教学信息，对教学中存在的问题及时向分院（系）、学院进行反馈。
5.教师—学生双向课堂教学效果反馈系统，每学期期中，由学生会组织学生填写
《课堂教学效果反馈表》，对所有上课教师的教学效果进行反馈。同时，教师每学期应至少 填写一次《课堂教学信息卡》，将课堂教学过程出现的问题（如学生的学习效果、学习风气、教学条件、教学设备的使用情况）反馈给学院督导。
6.网络教务反馈系统，通过网络获取教学信息。
为了达到全面控制教学过程、提高教学质量的目的，进行课堂教学检查时，各类检査人员应填写相应的评估表和反馈表，及时对评估表和反馈表进行统计处理，将结果反馈给教师 所在的教研室，并以适当的方式反馈给教师。每学期以分院（系）为单位，综合各种渠道 的检查结果和反馈结果，采取先定量后定性的办法，对所有任课教师的教学效果和质量进行评价。评价结果经分院（系）审核后，将结果存入教师教学工作档案，作为教师晋职、评优的重要依据。每学期，学院教务处对教学质量方面存在的共性问题采取简报、总结等形式，对存在的个性问题采取座谈会、个别交流、文字材料等形式，以随时总结经验，改进教学。

七、课程考核与评价

本课程是专业必修课程，考核方式有多项内容组成，期初就对学生明确。期末成绩为综合评定，由考勤（10%左右）、课堂表现（10%左右）、课堂作业（20%左右）、期末笔试（60%左右）等项目组成。

八、课程负责人及教学团队

课程负责人：董明

刘江苏,张扬

九、 其它说明

无

制定部门：智能信息工程学院 时间：2020-02-28

审 核 人： 董明 时间：