Research on the Teaching of "Vulnerability Scanning and Protection" Course Based on Individual Training

Guofang Zhang

Hainan college of software technology, Qionghai 571400, Hainan, China

Abstract : How to cultivate talents who master information security technology for society has also become a major task for universities. As a technical course in information security in vocational colleges, "vulnerability scanning and protection" faces many problems in classroom teaching. How to design classroom teaching and ensure that students are proficient in using the latest information security tools is the focus of this course. Based on the actual situation of classroom teaching in vocational colleges and the cognitive patterns of students, this article analyzes the practical problems faced in the teaching of the course "Vulnerability Scanning and Protection". Combining with the actual situation of classroom teaching and the learning situation of information security majors in vocational colleges, it proposes curriculum design strategies for practical teaching and designs practical teaching links to solve the problems in practical teaching, providing reference experience for the teaching reform of the course "Vulnerability Scanning and Protection".

Keywords: Strategy; Vulnerability; Scanning; Teaching.

《漏洞扫描与防护》教学中的问题与对策研究

张国防

海南软件职业技术学院，中国·海南琼海 571400

摘　要：高校如何为社会培养掌握信息安全技术的人才也成为高校一项主要任务。“漏洞扫描与防护”作为高职院校信息安全专业技术课，课堂教学中面临着诸多问题。如何设计课堂教学，学生熟练使用最新信息安全工具是本门课程的重点。针对高职课堂教学实际情景以及学生的认知规律，文章分析《漏洞扫描与防护》课程教学中面临的实际问题，结合课堂教学的实际情景与高职院校信息安全专业学情，提出实践教学环节的课程设计策略并设计实践教学环节，解决实践教学环节的问题，为《漏洞扫描与防护》课程教学改革提供借鉴经验。

关键词：策略；漏洞；扫描；教学

1 引言

高职院校信息安全专业的教学涉及很多新工具新技术，不同于其他专业的课程那样自成一个闭环知识体系，计算机网络开放性，可以让不同网络设备制造商的产品只要遵从网络接入协议的标准要求都可以接入，不同软件开发商的软件只要符合软件开发的要求都可以在网络设备中运行，互联网已经成为一个集合多款设备和软件的网络。由于网络中的设备、软件和策略都是由不同的开发者开发，由不同知识背景的用户使用，因此在互联网上会出现各种各样的漏洞，这些漏洞有些是设备自身引起的漏洞、有的是软件的原因引起的漏洞，更有一大部分是用户的失误造成的漏洞。仔细对这些漏洞进行分类，由硬件引起的漏洞称为硬件漏洞，由软件引起的漏洞称为软件漏洞，由用户的失误造成的漏洞称为用户漏洞[1]。这些安全漏洞越来越成为网络安全界关注的焦点，高校如何为社会培养掌握信息安全技术的人才也成为高校一项主要任务。“漏洞扫描与防护”作为高职院校信息安全专业技术课，课堂教学中面临着诸多问题，其中最主要的有缺少实验环境、没有合适教材、不能够实时更新；

基金项目：本文系海南省教育厅高等学校教育教学改革项目基金资助，项目编号：Hnjg2023-182.

学生基础差，学习积极性不高。如何设计课堂教学，让学生培掌握最新信息安全技术是本门课程的重点。通过分析《漏洞扫描与防护》课程教学中面临的实际问题，结合课堂教学的实际情景与高职院校信息安全专业学情，提出实践教学环节的课程设计策略并设计实践教学环节，解决实践教学环节的问题，对高职院校课程教学改革提供借鉴经验[2,3]。

2 现状和问题

高职院校信息安全专业的技术课程主要以网络信息安全为授课内容，因为网络是由硬件和软件共同组成的，并且由于客观的因素，网络硬件产品在使用中遇到客观的因素出现故障，这种由于网络硬件物理因素造成的故障也是导致网络不安全的一个因素。如果说网络硬件设备是网络的骨架，那么运行在网络硬件上的各种操作系统就是网络的灵魂，其它的各种应用软件就是网络的各个功能组织部分，由于软在开发时受开发人员的专业知识、安全意识和逻辑思维的影响，造成了软件隐藏着很多漏洞，在信息安全领域流行着一个共识：“所有软件都有漏洞，而且软件越大、漏洞越多”。由于接入网络的设备繁多，很多网络使用者由于网络安全意识不强，在使用中很容易留下安全隐患。这就导致网络中的漏洞一部分是网络设备硬件导致的，一部分是各种软件导致的，还有一部分是由于使用中人为错误导致的。从高职院校的课堂教学角度看，课程所学的安全漏洞主要是指各种应用软件所产生的漏洞。由于漏洞的隐蔽性，在漏洞被发现并不能及时被公布出来，所涉及的知识点何技能更是无法及时被公布，所以最新的漏洞往往不能够在高职课堂中学习，信息安全教学的知识和及时更新比较慢，而且落后过时。往往课堂上所学习的新的安全知识和技术已经被更新，旧的漏洞已经被新版本的软件修复。并且由于高职学生的学习能力导致在进行信息安全专业课程学习时的学习力度不够深入。总体上，信息安全专业课的教学面临的主要问题如下：

2.1 缺乏合适的专业教材

高职院校信息安全专业缺乏合适的教材是一个普遍现象，即便是市场上有一些教材，打都只是对信息安全泛泛而谈，大部分都是介绍些安全概念，总览整本书籍各章节题目，似乎很专业，但细看每一章节，都是长篇的概念性理论和一些代码。缺乏这些代码使用的实验环境，这些代码大都是通过网络搜集的，而教材并没有详细的准备实验环境，大都是为了体现专业性而写进教材，并没有考虑到高职办学教学的以使用为主的目的。由于漏洞大都是黑客首先发现的，黑客利用掌握的技术和工具对网络进行扫描，当发现一个存在的漏洞时，经常秘而不宣，私下独享或者在黑市进行非法交易获取利益，等漏洞被公布需要好长时间，缺少相关的人才及时将新的漏洞编写如教材，黑客更不愿将所掌握的漏洞及漏洞利用工具写入教材，教材不能及时更新最新漏洞是一个现实问题。另外，因为安全漏洞所涉及的技术和工具比较复杂，大都是国外首先发现并在发现者圈内流行一段时间后才传到国内，国内的的安全测试工程师还需要学习消化吸收，然后在将这些漏洞技术公布出来需要一些时间，这也导致了教材往往滞后新技术的发展变化，缺乏新技术新思维，课堂教学不能引起学生探索漏洞的欲望。

2.2 实验场景难以仿真

“漏洞扫描与防护”是信息安全专业的一门专业技术课，这门课程专业技术性很强，需要进行很多有一定难度的实验，如何在高职院校的实验室环境下搭建仿真训练场景，让学生能够得到一种身临其境的体验感是激发学生学习兴趣的重要因素，但由于许多漏洞都是在实际生产网络环境中被攻击者首先发现并利用的，这些网络攻击者并不是为了网络安全技术去交给外界的，而是将自己首先发现的漏洞和安全技术秘而不宣，漏洞产生的场景不能为外界所知，课堂教学更不可能取得这些漏洞的应用场景。又因为漏洞产生的实际网络环境非常复杂，常常有多种设备部署，而这也是课堂教学环境所缺乏的，在课堂或者实验室环境中难以完全搭建并仿真实际网络环境中的漏洞利用场景，这也是造成了课本知识与实际的东西脱节。并且许多漏洞的利用不仅需要掌握扎实的编程和专业的网络基础知识，还需要掌握一些网络工具并能够熟练使用，因为要熟练使用这些工具需要足够的时间进行反复的专业训练，这对于高职院校的学生来说具有一定的难度。这就造成了这门课的实践教学不能够百分之一百的仿真，学生的真实体验感不足，无法激起学生学习的积极主动性。

2.3 学生的知识背景参差不齐

高职院校的学生生源来源比较广泛，主要分为以

下几类：①参加高招入学的学生，这类学生都是经过三年高中学习，参加高考进入学校的，有一定的基础知识，能够自主学习，但这类学生有一个特点，对职业技能课还采用高中阶段那样的方法进行知识记忆，就为了这门课不挂科，能顺利毕业，面对安全专业课的枯燥理论，甚至在课堂上学习英语，为专升本考试，目的很明确。②通过单招入学的学生，这类学生以职业中专或者职业技校，甚至还有往届的高中毕业后参加工作多年或者服过役退伍后又来提升学历的，单招的学生生源宽广，学习经历和知识背景参差不齐，他们的上学目的又不同，在学习漏洞扫描这门专业课时的态度和学习能力差别很大，或者有个别感兴趣的学生由于知识背景和教育经历的原因，学习上有一定的难度。③五年一贯制学生，这类学生是初中毕业通过中考进入高职院校的五年制学习，他们在学校前面三年学习文化课，后面两年学习专业课。在学校的前面三年已经对学校的学习生活环境熟悉了，由于年龄小，有的学生比较贪玩，有的很爱学习，呈两极分化现象[4]。

2.4 数字化产品的影响

现在高职院校在籍的学生大都为 05 后，他们出生在数字网络通信时代，从小就受到数字产品的影响，对数字产品如计算机、数码相机、智能手机、笔记本电脑、IPad 等数字产品耳濡目然，拿来就会使用。又由于近年来教材教具的改革换代，从传统的黑板粉笔到现在教室的触摸屏显示器的变化，让这些数字原生代的学生习惯了快速接受知识，习惯于利用网络寻找资料，尤其是网课这种新的的学习方式，更深刻地改变着人们对学习的传统认知。高职学校的学生大都来自省内和省外，都是住校学习，每个学生都拥有自己的智能手机和电脑，由于学生所处的年龄阶段认知还不成熟，容易受到网络上的小说、游戏和影视的影响，不能合理控制自己上网的时间，在宿舍、周末几乎是机不离手，甚至是课堂上也在不停地刷手机，导致睡眠不足，课堂上注意力不集中，老师在课堂上讲的东西下课就忘，听课效果很低，实验课更是由于看手机导致的分心走神，忘记实验步骤无法按时完成实验[5]。

3 解决问题的思路

面对《漏洞扫描与防护》课程中诸多的现实问题，本文借鉴国家部队对士兵进行的个体军事素质训练思想，将每一种网络安全工具当作学生要掌握的科技武器，每一种漏洞作为一个训练项目，针对每一个漏洞，设计漏洞的知识背景和知识结构模块，在进行单个项目训练之前，要求学生了解并掌握给漏洞的知识背景以及应用场景，对每一个网络安全工具，设计该工具的知识背景及特点模块，学生在学习使用前都要了解工具的原理及特点，做到心中了然每种工具的原理及应用特点，以便在面临不同的工作场景时能够发挥自己的特长，做到对工具的超长发挥使用，激发学习和工作热情。按照漏洞 + 知识背景设计 + 网络安全工具 + 知识背景和使用特点对《漏洞扫描与防护》课程进行教学设计，每个训练项目设计不同的评价标准并实现评价标准的量化，课程的总体考核环节是综合每个项目的权重值，综合各个项目的权重作为本门课程的考核标准[6]。

4 解决问题的对策

4.1 重构课程知识体积和项目模块

根据“漏洞扫描与防护”课程的知识点重新构建课程知识体系，按照高职学生的认知规律划分课程项目，包括信息搜集、目标识别、端口发现，服务识别、漏洞扫描、漏洞验证、漏洞报告共七个项目，每个项目按照知识点又划分为若干任务模块，确定各项目的环境、工具、实验主机、数据库等内容。每个项目包含的知识点、所需使用的工具都详细累出清单，并将需要的工具打成资源包，放在网络指定的位置，方便学生实验室下载使用，课下也可以下载使用。对每个项目设置评分标准，以便学生在进行单项项目学习训练时对项目要求的知识背景和技能进行评估测试，达到学生可以自己对学习的模块进行量化考核的结果。

4.2 实验环节的虚拟化仿真

由于该课程的特殊性，一些网络漏洞与所处的网络环境和软硬件配置条件有关，这类漏洞只有在特定的网络设备和软件版本及硬件配置才可以利用，并且该漏洞没有被打补丁，需要在实验室里使用虚拟化技术进行仿真。因为受实验室条件限制，在高职课堂的实验室环境很难完全重现网络漏洞所处的真实环境。为了解决这些问题，本文采用虚拟化技术仿真实际网络环境，在虚拟环中搭建测试网络环境，部署测试目标靶机和渗透测试平台，并在渗透测试平台部署实验所需的各种工具，配置好虚拟网络主机的 IP 地址和服

务。将典型的漏洞渗透测试过程步骤制作成文档，当学生在该模块训练学习时根据实验文档能够顺利进行模块的训练学习。训练模块反复多次使用，直到学生完全理解并掌握该漏洞从发现到验证测试的全过程的步骤和技能。通过这种训练方式，学生可以对漏洞有深刻的认识并在训练过程中掌握了各种安全工具的使用，这对提高学生职业技能有很大的帮助。

4.3 设置阶梯的训练模块

由于高职学生的知识背景差异大，不喜欢枯燥的理论的特点，按照高职学生的学习力和认知规律对每个课程项目进行任务分解，并根据任务涉及的知识点的多少以及所需要使用的工具使用的难易程度划分阶梯课程模块，将课程模块按照难易程度分为低难度任务、中难度任务和高难度任务。实践课让学生先训练低难度任务模块，然后有能力的学生在掌握了低难度模块后再根据个人情况选择性练习中难度任务模块。个别能力比较强的学生在掌握了中难度模块，然后还可以选择高难度任务模块。每个任务模块都设置了评价标准，可以对学生掌握的知识点和技能进行测评。实践证明，这样设置课程任务模块能充分调动学生学习的积极性和探索钻研精神，符合因材施教的要求。很多学生从懒得动脑、懒得动手变成了乐于动脑、喜欢动手训练，可能有些同学是出于掌握一些必杀技以证明自己的能力，在参加各种比赛中以至于不落下风。

4.4 将手机使用状态纳入考核指标

现代的高职学生大都出生于数字产品时代，从小就接触计算机网络和智能手机等数字产品，尤其是每人一部智能手机都视若珍宝，手机中的抖音、朋友圈、小说、影视更是这些数字生的喜爱，其中一部分同学沉醉于手游，在宿舍经常刷手机到深夜，以至于影响休息，严重睡眠不足。学生课低头刷手机一直是高职课堂的一个问题，为此，在本文中把的课堂上学生的抬头率作为评价课堂教学的一个指标，在具体实施中，可以灵活变通，每节课结束时检查学生手机电量不失为一个小妙招，根据手机电量评价学生课堂手机使用情况，能够降低手机课堂使用率，提高了课堂抬头率，实践证明这种方法很有效。

5 结束语

由于高职学校是培养技术应用型人才为宗旨，因此高职院校的课堂教学不同于本科院校的课堂教学，高职院校课堂教学尽量减少理论推到，重点突出技术应用，作为信息安全专业课的漏洞扫描与防护牵涉的概念理论复杂并且逻辑抽象，从概念学理论的方法是行不通的，需要概念加技能实操才可事半功倍。

参考文献

[1] 高晓峰 . 漏洞你先知 电脑更安全 [J]. 计算机与网络 . 2016(13).

[2] 陈涛 . 基于网络的漏洞扫描器设计与实现 [J], 电脑知识与技术 2008.11.

[3] 官节福 . 计算机网络安全与漏洞扫描技术的应用研究 [J], 电脑知识与技术，2022.9

[4] 黄超 . 基于职业核心能力培养的网络安全课程教学改革 [J]. 襄阳职业技术学院学报，2018.7.

[5] 张国防 , 基于 web 页面的 SQL 注入研究 [J] 网络安全技术与应用 , 2019 3.

[6] 罗建桢 , 王勇等 . 高职院校应用型网络安全人才培养的教学方法研究 [J].2017.10.