高职院校的渗透测试技术课程的教学改革探索

张泽连
湖南信息职业技术学院

[摘　要]随着新时代网络信息发展，信息安全与管理专业相关课程需要积极尝试改革创新，探索适合高职院校的课程教学方式。本文结合本院背景深入分析《渗透测试技术》课程存在的不足，结合市场人才需求制定教学与实验内容，融合多平台的实验内容，采用多种教学方法，取得良好效果，受到学生好评。对新形势下的信息安全与管理专业相关课程的教学具有借鉴意义。

[关键词]渗透测试；信息安全；人才培养；多平台
【DOI】10.12252/j.issn.2096-627X.2021.12.792

引言

随着近年来网络的井喷式的发展，网络已经渗入到各行各业中，信息安全越来越重要。对于高职院校来说培养渗透测试工程师也是人才培养方案中重要一部分，该课程属于网络安全岗位课程，培养面向网络安全设备设计人员、网络安全渗透测试人员、Web安全管理人员、网络安全检测人员等。

《渗透测试技术》课程是我院信息安全与管理专业开设专业核心课程之一。渗透测试主要是在授权的前提下模拟黑客可能使用的攻击技术和漏洞发现技术对目标系统的安全作深入地探测，发现系统最脆弱的环节。课程通过渗透测试的小案例贯穿每个章节，培养学生如何对目标主机和目标网络进行安全检测与安全加固。本文从课程现状分析、课程目标、课程内容、课程改革、改革成效等几个方面展开探究。

一、课程现状

课程开展以来主要以教师教授，学生听讲加实践的单一教学模式，课程共 90个课时 15周，每周以“2+4”的模式即2节理论课对应 4节实验课，目前根据学生上课反应及考核情况，存在以下几个问题亟待解决：

第一，课程内容相对陈旧，目前针对高职院校的渗透教材不够全面，内容比较老旧，这部分理论知识和实践内容不能满足目前网络安全相关行业的最新需求。在国内比较优秀的渗透测试教材建设还不够全面，单独一本教学内容不能满足全部教学内容。目前我们选取的教材出版时间为2015年，很多工具已经被官网摈弃或者停止维护，教学过程需要教师从不同的渠道获得最新的资源。第二，教学平台单一，课程作为核心进阶课程，要求学生要有一定的基础专业知识，目前学生对前期课程掌握程度不一，专业水平能力也不尽相同，使用单一的实践平台教学，学生对课程的内容接受度较低，兴趣度较低，积极性不高。第三，教学方法不够新颖，课程教学主要按照传统的教师讲授、ppt演示、学生实操，不够灵活，不够全面，不能满足需求。

二、课程目标

课程目标主要以符合适用专业人才培养方案中的培养目标和培养规格的要求，制定以下三方面培养目标。

（一）知识目标

能够搭建DVWA漏洞环境、Kali Linux测试环境，熟悉Metasploit 工具进行渗透测试，能够应用各种漏洞对目标主机进行渗透攻击，熟悉常见的主机、应用、服务漏洞，能够实现内网和web的渗透。

(二)能力目标

通过“Kali Linux渗透测试”应用实践，培养学生能够使用nmap进行网络扫描和嗅探，灵活应用Metasploit进行渗透测试，能够进行暴力破解、命令执行漏洞攻击和能够进行内网攻击和web站点进行攻击。

(三)素养目标

通过本课程的学习，培养学生遵纪守法、热爱国家、家国情怀。培养学生独立分析问题和解决实际问题的能力，具有良好的团队协作精神；树立学生勤于思考、做事严谨、勇于创新的工作作风和良好的职业道德。

三、课程内容

课程共包括10个章节，结合企业岗位需求与最新技术制定教学内容，课程部分章节内容如下：

(一)初识渗透测试

熟悉网络安全的法律法规；熟悉渗透测试的基本概念；熟悉国际渗透测试流程渗透测试执行标准(PTES)；了解安全漏洞的生产周期；了解各阶段执行的相关工具及渗透方法。

(二)信息收集

了解信息收集的方法，能够较准确的完成对目标进行情报收集。熟悉使用被动在线收集工具 Netcraft，Zoomeye；掌握主动信息收集工具nmap；掌握被动收集工具whois查询、Recon-NG。

(三)漏洞扫描

了解漏洞的基本原理及漏洞扫描的基本概念及流程，能够运用工具对目标进行漏洞扫描，熟悉常见的漏洞类型；掌握漏洞扫描工具nessus、X-Scan、基于metasploit的专用漏洞扫描器。

(四)渗透攻击

利用操作系统漏洞、目标欺骗手段进行渗透攻击。熟悉多种渗透攻击工具，实现对目标进行渗透攻击；攻击成功后收集目标系统数据并清除踪迹，最终创建持久后门。

(五)社会工程学

熟悉社会工程学攻击特征，熟悉基社会工程学工具实现目标攻击；熟悉社会工程学攻击防御的方法。

(六)web渗透之SQL注入

熟悉SQL注入原理及方法，能够自行搭建dvwa靶场，通过对模拟站点分析识别SQL注入点，掌握基本的SQL注入的防御方法。

(七)Web渗透之XSS

熟悉XSS攻击的原理及方法，能够在靶场进行XSS漏洞攻击，通过修改靶场安全级别，能够绕过对应的过滤机制，并分析XSS攻击防范方法及手段。

(八)Web渗透之文件包含、文件上传

熟悉文件上传和包含攻击的原理及方法，能够对目标网

站进行文件上传、包含漏洞攻击及利用，能够熟练使用burp suite工具截取数据包、修改数据包、密码爆破，使用中国菜刀拿到webshell，对目标网站执行相应的绕过测试。掌握文件上传、包含的攻击的防御方法及手段。

(九)Web渗透之命令执行

熟悉命令执行攻击的原理及方法，能够对目标网站进行命令执行攻击，能够利用该漏洞查看目标系统的隐私文件、查看服务器日志文件，生成shell等，掌握命令执行攻击的防御方法及手段。

(十)综合实践

以项目的角度熟悉一个渗透测试项目所包含的全部内容，从竞赛视域设计项目，分组分角色相互协作完成一个渗透测试项目。

四、课程改革

针对目前课程的现状及存在的问题，以企业岗位需求为导向，从教学内容、教学资源、教学实验平台、校企合作、教学方法等多方面进行教学改革。

（一）确定教学主题，更新教学资源

针对目前课程资源陈旧的现状，引入了多元化的教学资源，用线上线下混合模式教学。线下内容主要以教材为主，线上资源主要包含超星学习通、B站、CSDN、51论坛等多个渠道内容，教师在学习通上创建了本课程的在线课程，导入所教班级，上传教学资源，包括教学视频视频、教学ppt、实验文档、题库等，同时在对应的章节导入 MOOC和 B站点的相应链接。实验教学过程中，通过实验环境模拟对已授权某公司内网服务器和web站点做渗透，将案例分解为小案例，按照渗透测试标准的8大阶段开展教学，包括前期沟通交互、信息收集、漏洞扫描、漏洞利用、后渗透攻击、社会工程学、web渗透、渗透测试报告。每个阶段根据教学主题从多种渠道整合教学资源，包括最新理论和最新工具等实践内容。这个阶段通过更新教学资源，扩展了现有的资源库，增加了学生的知识面，同时最大限度地将教学内容与社会最新岗位需求相吻合，为学生就业做好精准对接。

（二）多种平台相融合，开展实践教学

为了达到的更好的教学效果，在高职院校采用多种平台相融合的教学方式。

1.传统实验环境，简单的实验按照传统的渗透测教学在物理机上安装VMware Workstations，并安装多个虚拟机，为每台虚拟机设置不同的角色，包括攻击主机和目标主机，kali linux担任攻击主机，kali上集成了多种攻击工具，windowsXP或者win7担任目标靶机，目前很多教材都是使用这种环境，拥有一台普通pc机就可以在授权的情况下完成渗透。但是该环境对计算机的要求比较高，处理器至少要I7以上，内存4G以上，虚拟机在运行过程中还需要占用一定的硬盘空间，学生在操作过程中容易出现卡顿或者死机的情况。

2.对于web渗透，通过在虚拟机中搭建dvwa靶场，能够对SQL注入、XSS攻击、文件上传、命令包含、命令执行子案例多个子案例进行基本实践练习，通过实践来熟悉各种web渗透攻击的原理及攻击方法。

3.引入360校企合作网络安全实践平台。对于复杂的拓扑步骤较多的内网渗透实验采用平台案例，比如后渗透攻击中清除日志，通过跳板控制目标机，平台上的设备及服务器较为稳定，硬件条件较为良好，能够保证案例中涉及的知识得到更好的练习。Web渗透实践内容平台有自有的靶场，教学过程中将步骤较多，工具繁杂的案例，教师通过平台下发任务给学生，学生以学生角色登录平台，此部分内容属于进阶内容，对于专业基础较强的同学可以完成该部分内容，如文件上传这一章节，学生可以可绕过平台靶场的安全级别限制，通过burpsuite工具的修改数据包，并通过中国菜刀和中国蚁剑拿到目标站点的webshell，同时可以拿到目标机的控制权限。

4.引入360补天、漏洞盒子平台，以竞赛演练的视角完成实战任务，按照 6人一组完成平台项目，组内分为小组长和组成员，每组撰写渗透测试方案 1名，实践操作的人员 4名，文档整理 1名，最终由组长提交相关实践文档，并将操作过程遇到的问题进行归纳和总结。考核按照小组之间互评给分，最终教师给出评价，这个阶段让每位学生都参与到实践中，模拟企业项目组，按照学生兴趣和能力分工合作，各司其职，提高了学生的沟通协作能力，培养了学生的职业能力和动手能力。

（三）多种教学方法相结合

教学过程中除了采用传统的教师讲授、演示，还借助大量的多媒体资源进行案例分享，还采用了分组法，分层式教学法，翻转课堂[3]，攻防演练等多种方法，通过多种教学方法，增强了学生学习兴趣，提高了专业技能，取得了较好的效果。

五、效果分析

从多方面可以印证教学效果良好，首先在期末考试成绩及格率超过90%，优秀率65%，其次在后续《项目设计与开发》课程中能够将内网渗透与web渗透作为毕业设计选题的超过40%。再次，部分学生能够在360补天及漏洞盒子挖到漏洞并获得证书和奖金。最后通过调查问卷形式统计到以信息安全作为个人职业发展方向的比例较之前提高23%,可见学生对于渗透测试技术呈现浓厚的兴趣，专业知识迁移能力和独立动手能力得到了提高。

六、总结

《渗透测试技术》课程使用本文的改革方法开展教学，丰富了教学资源，提高学生的知识面，多实验平台提高学生的实践能力，提高了学生的兴趣与职业认同感，有较好的教学效果。教师不断探索课程教学改革的同时也需要顺应时代潮流，提高自身的综合素质，将更多的知识传授给学生，为国家培养更优质的网络安全人才。

参考文献：

[1]罗利.大数据专业Hadoop开发技术课程实践教学探索[J].电脑知识与技术,2021,17(12):110-111

[2]黄为.计算机网络渗透测试技术探究[J].网络安全技术与应用,2021(12):8-9.

作者简介：张泽连（1986-），女，湖南长沙人，助教，硕士，湖南信息职业技术学院助教。主要研究方向：计算机网络技术、信息安全与管理。