高职院校网络安全课程教学研究

宋　伟　黎银环
（江门职业技术学院信息工程学院，广东 江门 529000）

摘要：“没有网络安全就没有国家安全”，当前网安人才的培养被提升到了战略发展的高度，随着国家越来越重视及网络安全的人才培养，以及重视当前职业教育的改革，职业教育如何培养出适合自己体制的网络安全人才就成为了一个研究的热门，本文就职业教育如何才能培养出合格的网络安全工程师做出具体的研究探讨。

关键词：网络安全；人才培养；职业教育

疫情祸乱和俄乌战争给当前的世界带来了动荡不安的局面，媒体的揭露让我们看到了一个全球祸乱的根源地－美国，随着360公司于期揭露了西北工业大学被攻击的真相，让我们看到发展网络安全人才是迫在眉睫的事情，美国、俄罗斯以及西方国家在网络安全人才培养方面已布局多年，相对而言，我国对网安人才的培养重视相比滞后。

这几年国家大力发展网络安全，把网安人才的培养上升到了国家的战略发展高度，“没有网络安全就没有国家安全”，一时国内掀起了各种举办网络安全赛事的热潮，为的就是培养出更多的网安人才。

本人曾在联想、电信集团大企业从事一线网络安全工作，广东省等级保护专家，知名黑客团队MS08067成员，入校从事本职工作后作为指导教师曾指导学生参加过各类网安大赛，获得过全国职业技能大赛国家二等奖以及相关奖项十几项，成立了校内网络安全实验室eyaslab，带领学生团队主办了校内“第一届雏鹰杯网络安全大赛”，积累了丰富的竞技和教学经验，现结合当前高职教育网安人才培养的现状将个人的见解和经验分享如下。

一、目前存在的问题

（一）人才培养定位问题

高职院校的网安人才培养目标很多还是定位在理论型人才的培养，以PPT教学为主，学生能够明白一些网络安全的原理，实践动手经验存在着严重不足的现象，我们称之为理论型网络安全工程师，这一类型与企业的人才需求存在着明显的脱节问题，满足不了需求。

（二）教材问题

教材的选取目前多半还是采取一些理论型教学书籍，一些高职院校选取教材时有要求必须选用一些国家规定的十四五等规划教材，但这一类的教材中不一定就有适合教师自身特征的书籍，也不一定就满足了学生的实际需求，网络安全技术发展可谓日新月异，有些教材从编写到出版，再到被教师学习，再到传道，这本身有着一些周期，难免可能会存在着跟不上时代的问题。

当然，也有一些教材可能可以满足需求，但因为教师自身不熟悉这类技术的原因，所以选材时被忽略，毕竟化繁去简是教学中的一种必要趋向，如果教师都觉得非常难，那么在传授给学生时势必也是一个难题，难保不会遭到否定。

（三）实验环境问题

一是实验环境依赖教材指定，很多都是单机环境，工具老化单一，有些甚至是十几年前的工具，攻击思路单调，所获较少，缺乏灵活度和扩展性，针对网安专业的发展特色相比较，太为落后。

二是依赖安全公司，一些学校校企合作建立了相关的网络安全实验室，具有一些相关的实践平台和教学环境，教师熟悉相关资源之后可以分配给学生，但该环境也存在着无法更新和快速老化的问题，过几年就跟不上时代，再次建立需要较大的开支，而大多数高职院校并不能及时的获得更新资源的发展条件。

（四）师资问题

缺乏实战经验的教师是高校普遍存在的问题，经验丰富的黑客多半都在企业一线，他们依赖自身高超的技术可以获得丰厚的回报，而扎根在高校的数量就比例相对很小，很多高职院校想吸引相关人才是非常困难的，那么如何吸引或者培养出实战经验的教师是一个待解决的难题，毕竟教学规律还是遵循着木桶原理，最短的那一块决定着最终发展的高度。

另一方面就是高职院校也缺乏自身师资提升的条件，教师的进修依赖于学校资源的分配，教师可以参加一些指定的进修，比如省培和国培，但该类培训通常满足不了提升的实质性需求。

（五）教学方法问题

目前的教学方法还存在着手段单一的问题，PPT理论教学，单机软件实践，且实践是照着书本要求来完成，缺乏像样的靶机系统，得不到有效的实训效果，且课后缺乏训练资源，或者指导不到位，如何丰富课堂教学和课后练习，这也是网络安全课程教学的一大问题，这决定着最终的训练质量，没有着优质的训练资源，人才培养只是一个口号。

二、修改优化建议

（一）人才培养定位优化

与企业的实际需求相结合，与国家的人才定位相结合是目前高职院校网络安全课程教学要解决的问题，高职院校的学生存在基础差，学制短的问题，2.5年在校时间，除去第一年的公共课学习，那么真正学习专业课的时间只有1.5年，所以这么短的时间内，我们要将发展的定位为渗透测试工程师较为合理，这一点本人使用了8年实践教学结果进行了佐证，效果较为理想。

具体就是将课程内容定位windows系统渗透、LINUX系统渗透、软件渗透、web系统渗透、代码审计，python安全攻防基础，使学生在学习后能够掌握一些主流网络安全系统和软件的使用，如kali linux攻击系统，工具如nmap、burpsuite、awvs，sqlmap，nikto，metasploit，nessus，meterpreter，cobalt strike等等，也会去

攻击一些具体的目标，能够拿下 web 系统，掌握 owasp top 10 类型漏洞的攻击手段，进而可以逐步成长为白帽子黑客，而难度较大的灰帽子和黑帽子人才定位就不适合。

（二）教材问题选取建议

教材的选取不局限于十四五等规划教材，可以考虑采用一些优秀的其他出版社教材，比如 MS08067 实验室出版的《web 安全攻防 – 渗透测试实战指南》《python 安全攻防 – 渗透测试实战指南》等，或者可以采用优秀的黑客编写的未出版的电子版书籍如红日安全团队编写的 web 安全系列、PHP 代码审计系列，详见 https：//xz.aliyun.com/u/10394，如果有校企合作的高校也可以考虑采取合作企业编写的优秀教材进行教学。

（三）实验环境问题的解决

实验环境缺少是目前发展的一大短板，一些已经建立校企合作的企业可以采用购买的堡垒机等相关资源，没有实验环境的需要教师自身进行收集或者搭建，目前互联网上可以收集到的资源已经很多。

比如 windows 攻防可采用魔鬼训练营提供的具有 MS08067 漏洞攻击靶机系统，或者 win7 任意版里的 MS17–010 漏洞，当然还有一些包含了其他 WINDOWS 系统漏洞的系统都可以拿来使用，攻击成功之后可以在此基础之上继续进行下一步的实操训练，如 meterpreter，cobalt strike 讲解的是配合攻击之后如何进行进一步的提升权限，关闭防火墙，打开摄像头，打开远程桌面，复制拷贝资料，移植进程，安插后门程序，跳板程序，清除日志等一系列后续操作以提高学生的系统化训练成效。

linux 攻防可采用知名的弱点测试系统 metasploitable2（linux 漏洞集 +WEB 漏洞集），此系统是开发出大名鼎鼎的 metasploit 工具集的知名的黑客团队所作，目前已经有 3 个版本，其中 metaspolitable 第 1 版因为出产较早，一些知识已经过时，不过还是可以拿来训练，而 metasploitable3 需要自身来搭建，且网上没有关于该版本的系统化攻击教程，所以这些对于经验不是非常丰富的老师和学生都还是有些难度，可以考虑作为课后训练资源进行提供，而 metasploitable2 底层是 ubuntu9 版本系统，有着为数众多的系统漏洞和软件漏洞，网上可以找到相应的攻击教程。

web 渗透也可采用 metasploitable2 来进行训练，它集成的 web 漏洞系统也较为丰富，如 dvwa 系统，这套系统是专门用来训练 web 里面的 owasp top 10 类型的漏洞攻击，有着低中高三个难度等级，且网上有着相关的通关秘籍，可以拿来深入学习和训练，除了 dvwa 之外还有 wordpress 等漏洞系统，都可以给学生拿来做课后训练资源进行拓展。除了 metasploitable2 之外我们也可以采用 github web 漏洞靶机系统，详见 https：//github.com/c0ny1/vulstudy，上面讲述了使用 docker–compose 工具一次性搭建多个靶机平台环境的详细教程，可以满足课后的训练资源。

为了提高训练效果，学校每年会选派学生参加为数众多的职业技能大赛，以赛促学，那么如何训练学生参加竞赛也需要平台来训练，竞技平台也可自行采用 CTFD 或者 FBCTF 进行搭建，去 github 收集开放的竞技资源进行赛事还原，当然这个环节通常需要经验丰富的老师和学生来牵头完成，除了 CTF 训练还需要对抗平台，AWD 对抗平台搭建可采用开源的 cardinal，H1VE，AOiAWD 等，也可以利用线上资源如 bugku 平台。

（四）师资培养问题的解决

师资的缺乏是发展的最关键问题，参照一下现在的网安人才公务员招揽机制，公安部、公安厅、公安局在人才引进方面都采取了破格的条件，学历和技术水平达到要求可免试入公务员体制，而高校相对而言还是较为保守，以职称为第一要素，这难免会影响到人才的引进，当然这是个难以解决的难题，此处不作探讨。

那么剩下的一种方法就是从自身培养角度去出发，目前虽然高校每年都有组织教师参加国培和省培，但收效甚微，原因在于很多组织这个培训的机构没有设置相应的培训内容培养符合高校发展需求的人才。所以，学校应该资助教师去参加一些具有真正实战的机构去进修，并拿到相应的专家认证，如 360 和国家安全测评中心的渗透测试工程师 CISP–PTE 认证，注册渗透测试专家 CISP–PTS 认证，注册应急管理专家 CISP–IRE 认证，国际化的 OSCP 认证等等，只有这样，才能真正地解决高职院校网络安全教师的匮乏问题。

（五）教学方法问题的建议

网络安全人才的教学必然是以实践为主，理论为辅，高职院校学生可塑性强，有了足够多的实战，一切自然水到渠成，我们可以借助于一切可利用的资源来进行教学，比如 3.3 里面提到的一些资源，这当然也需要教师自身先要熟悉和精通这些技术，课堂实战演示和指导，课后给予训练建议，每年的校园技术节可以组织学生搞一次攻防竞技，也可组织学生参加各种类型的竞技，以赛促学是最好的手段。

三、发展前景

目前网络安全人才的缺口非常大，培养我们的网安大军人才巩固国防安全是当前迫在眉睫的事情。国家对职业教育的发展重视也达到了空前的高度，给予职业院校的发展上前所未有的支持力度，高职院校要搞好网络安全的教学必须有着清晰的定位，重点就在于培养白帽子黑客人才，与本科层次的人才培养相区别，适合自身发展的才是最好的。

参考文献：

[1] 付详，从职业竞技角度进行网络安全课程改革的实践 . 机械职业教育，2014（12）：44–46

[2] 黎银环，宋伟，以技能竞赛促进高职计算机网络技术专业人才培养 . 广东教育 . 职教，2018（3）：29–31

[3] 张丽敏 . 基于云计算技术的网络安全攻防实验平台设计与研究 . 电子设计工程，2018，26（17）：62–65

[4] 侯海燕，赵鼎，白光安 . 信息安全攻防实训平台的设计与部署 . 科技视界，2016（19）：238，281

[5] 宋伟，黎银环，高职院校网络安全竞赛系统化训练研究 . 福建电脑，2020（3）：50–51