聚知刊出版社
JZK publishing

司法信息安全专业实验平台设计与搭建

冯平

武汉警官职业学院，湖北武汉，430079；

摘要：大数据时代的来临，互联网、电信网、广播电视网、工控物联网等专用网络相互集成融合，网络安全威胁也从虚拟网络空间快速渗透到实体空间。新形势下，司法信息安全专业迫切要求建立一个崭新的网络专业人才培养体系，培养急需的高质量、实用的各类型信息安全专业人才，建成面向行业和工程领域的信息安全实践平台则显得尤为关键。为司法行政系统培养一流网络安全人才，建设完整的、标准的针对不同教学对象的高水平的信息安全实验室，对院校自身的教学和发展，对产生良好的社会效益，均有重大的意义。

关键词：信息安全；司法信息安全；司法信息安全实验平台

DOI：10.69979/3029-2735.25.11.079

引言

在高度数字化的今天，各行各业的数字化、网络化、智能化程度越来越高，各类生产活动创造出大量有价值数据，存储在各个数据中心，一旦出现网络安全问题，将会给产业和社会发展带来显著影响，甚至会引发国家社会层面的安全风险。近年来勒索病毒、震网病毒、西工大被网络入侵等重大安全事件接踵而至。随着技术的不断进步，网络攻击者的攻击成本不断降低，同时攻击方式更加多样化、隐蔽化，这些造成了各类信息安全事件频发的主要原因。近年来，国内的信息安全发展需求十分迫切，为司法行政系统提供信息安全人才的本专业是十分具有发展前途的特色专业。

1 司法信息安全实训室建设的目的和意义

司法信息安全专业掌握的专业知识和技术技能，面向监狱、强制隔离戒毒所信息技术岗位，培养能够从事监所信息系统安全保障、运行维护等工作的高素质技术技能型警务人才。专业的核心课程主要有《监所信息网络建设与维护》、《服务器配置与安全管理》、《计算机网络攻击与防护》、《监所安防系统安全运维》、《信息安全管理实务》等。

本专业需要学生掌握丰富的信息安全理论知识，同时理论知识的理解与运用，需要通过大量安全实验来巩固，许多安全技术与手段需要在实践过程中去认识、去体会。在国内很多高校开设的信息安全专业都使用了各种各样的实训平台有效地支撑着该专业学习。而目前我校司法信息安全专业缺乏有效的实训教学平台。该课程的教学方式主要以传统讲解为主，并辅以 PPT 等形式给以演示，或者利用一些简单工具进行练习。偏重理论知识的传授，并不强调实际环境的运用能力。组建一次实验课的成本大、花费时间长，且实验内容单一而且彼此相对独立。

司法信息安全是一个面向行业、面向工程的专业教学领域。司法行政系统、监狱戒毒系统近年来信息化的发展迅速，司法大数据云平台、监所数据库信息系统等支撑着司法行政各项业务有效运行，随之而来的安全性问题应运而生。司法信息安全专业急需一个面向行业业务、各工程领域的实践平台，加深对信息安全理论知识、行业业务理论知识、及信息安全实践原理的认识。这样能有效培养出适应行业、适应市场需求、适应具体工程应用的专业司法信息安全人才。

2 司法信息安全实验平台的实验项目分类

信息安全体系结构与计算机网络分层原理类似，将信息安全的大框架分解成若干个层次去完成相应功能。根据国家计算机安全规范，信息安全体系大致分为以下五个层面：

实体安全，包括机房、线路和主机等设备的安全。

网络与信息安全，包括网络的畅通、准确以及网上信息的安全

应用安全，包括各种程序开发及运行、数据库系统等的安全

系统安全，包括各种设备上运行的操作系统 linux、windows 等的安全

内容安全，包括非法的、有害的信息内容在网络中传播等

根据信息网络安全体系结构的五层分析，结合网络

攻防技术的实践与密码技术应用、网络安全应用理论部分知识，司法信息安全实验内容主要分为信息系统安全、网络安全、密码学与应用等 7 个类别，每个类别按照知识体系结构，又可分解为若干个实验内容,具体如表 1 所示。

表 1　司法信息安全实验项目分类

实验体系	实验内容			
密码学与应用	密码学	密码学应用	PKI	PMI
信息系统安全	应用系统安全	linux 系统	操作系统安全	数据库安全
	身份认证	计算机病毒分析实验	安全审计	容灾备份
网络安全	安全风险评估	web 安全实验	网络安全实验	网络攻防分析
	防火墙	入侵检测	VPN	漏洞扫描
	网络扫描与嗅探	密码破解技术	数据库攻击技术	网络欺骗技术
	系统安全策略配置技术	网络设备攻击技术		
数据内容安全	教据保密与安全	隐写软件安装及使用	水印攻击实验	信息隐藏
	数字水印			
软件安全	缓冲区溢出技与漏洞分析	恶意代码分析	逆向工程技术	软件安全测试实验
	软件安全防护	源代码安全审查	软件水印	
信息安全工程实践	安全编程	综合实验		
计算机取证与司法鉴定	LINUX 系统的计算机取证	windows 系统计算机取证	电子数据司法鉴定	

3 虚拟信息安全实验平台的分析

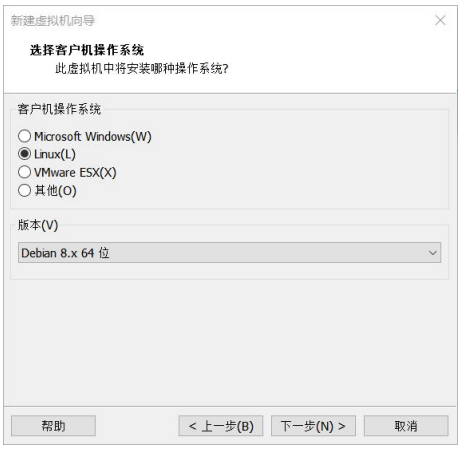
目前信息安全实验平台的搭建主要有两种方式，一种是在传统实训机房自行搭建实验环境，另一种则是购买现有信息安全服务厂商（如：360、深信服等）已开发的市场应用成熟的信息攻防实验室平台。

自行搭建实验平台需要较好的硬件和软件环境支撑，硬件环境上需要具有较强配置的单机，物理内存建议 16g 以上，存储设备建议在 1TB 以上，CPU 建议 8 核以上，因为单机上需要运行各种虚拟软件如 VM Ware,Virtual box,Cisco Packet Tracer 等。虚拟机中同时运行多个操作系统，可以扮演攻击机、靶机、代理主机、NAT 主机、服务器等多种角色。一些网络设备如：路由器、防火墙、IPS 等既可以购买物理硬件，也可以由学生通过搭建虚拟硬件的方式来实现。实验平台采用自搭方式步骤较复杂，对学生初始学习时，难度要求较高，但后期学习遇到的阻力会渐少。每类实验的实验环境需要学生灵活去搭配，准备工作时间长，学习中碰到的问题往往需要自行调试解决，缺少过程引导，需要任课教师介入的内容多。但可以让学生全方位的学习到信息安全的理论和实践各环节的知识。

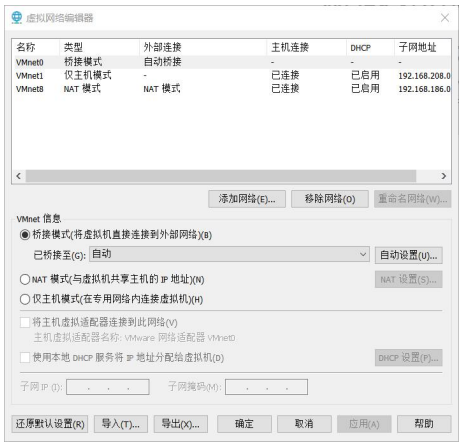
现有安全服务厂商的信息攻防实验室产品经过市场的检验和测试，在易用性和稳定性上相对于自建平台要更优秀。注重网络攻防学习的体系化建设，通过建设“学、练、考、评”一体化平台，以攻防训练为核心，以任务目标为导向，集知识培训、技能训练、能力考核于一体，提供种类丰富、配套齐全的精品课程和贴近攻防实战的技能训练，通过智能化数据分析，形成完备的人才能力评价体系，对网络安全人才进行可持续性、系统化的培训。平台的搭建上，主要通过购买云平台或者厂商的专用安全设备实现。通过多台专用信息安全虚拟化设备，虚拟出信息安全所需的场景，例如 WEB 攻防平台、应用攻防平台、威胁分析平台、数据挖掘平台、基线扫描平台、漏洞分析平台、木马分析平台等。同时系统提供相实验指导书和实验环境场景。学生前期学习难度低，无需考虑过多的前期的环境搭建上，过程实现上依据实验指导书有序进行，教师只需关注理论知识的讲解和相关实践内容的串联即可。

4 司法信息安全专业实验平台的设计与搭建

根据对以上的两种信息安全实验平台搭建方式的分析，两者存在着各自的优势和不足。自行搭建方式经济成本相对低。教学难度前期高，但后期效果好，更适合深层次学习。厂商的“学、练、考、评”一体化平台，教学难度比较适中，学生只需专注于操作原理和实现过程，教师只需引导介入即可，适合信息安全学习的初始阶段。因此在信息安全专业的不同阶段，结合使用不同的平台效果最佳。专业基础课程《网络安全基础》、《网络安全概论》等课程，比较适合使用厂商平台。进入高年级核心课程学习阶段，《服务器配置与安全管理》、《计算机网络攻击与防护》等课程，则较适用于自行搭建平台的使用。下面以本人《网络攻防技术与实战》课程中实践教学所使用的实验平台为例，具体介绍司法信息安全专业实验平台的设计与搭建。



图一 虚拟机支持的操作系统



图二 虚拟网络交换机

因缺少信息安全实训平台，实际教学中要求学生在电脑中使用 VMware 或者 Cisco packet tracer 软件自行组建实训环境。Cisco packet tracer 可以模拟出路由器和防火墙等安全设备。支持做一些关于路由器 ACL 配置和防火墙的安全设置实训。VMware 可以模拟出 Linux、Windows 等多种操作系统的主机和设备，并自带有 VMnet0、VMnet1、VMnet8 等 3 个虚拟交换机。分别支持桥接模式、主机模式、NAT 模式。通过虚拟网络编辑器的设置，结合不同系统的虚拟机，就可以构造出不同的网络拓扑结构下的网络安全实验。使用一些开源的靶机平台（如 DVWA、Metasploitable、OWASP Broken Web Applications Project 等）也能够很好的支撑初学者的需求。攻击机和其他角色的服务器、网络安全设备也可以灵活配置。常见的网络安全实验的虚拟机角色如下：

攻击机：kali

靶机：metasploitable 2、原始版本的 Windows 7

Nat 主机：windows 2008 server

代理主机：kali 下 owasp zap,burpsuite

防火墙:windows 防火墙，或者 kali 下 iptables

漏洞扫描器: OpenVas 虚拟机

路由器、服务器等：window 2008 server 或者 Ubuntu

以漏洞扫描为例，端口扫描实验可以使用 kali 作为攻击机，windows7 作为靶机，在 kali 上使用 Nmap 工具对 windows7 的 445、80 等常见端口进行测试。服务扫描可以使用 metaspoitable2 作为靶机，使用 kali 下的 metasploit 中的 http_version、mysql_version 等模块进行服务软件版本的扫描。操作系统扫描则可以使用 OpenVas 虚拟机作为攻击机，以 metaspoitable2 或者 windows7 作为靶机，进行系统安全性测试。更加复杂的实验，可能需要两台以上的虚拟机参与。比如网络隐身中的 NAT 实验，需要配置内外网主机各一台，nat 主机则在 windows 2008 server 的路由和远程访问服务进行配置即可。

5 结语

通过使用虚拟软件搭建实训平台的方式，延长了网络安全实训环境配置的时间，但在对实训环境的布局过程中，教师可以融入实训原理和实训过程的讲解，不仅让学生知道如何去做，而且能够理解这样做的原因。在一定程度上提高了教学的深度，因课程教学课时的限制，教学进度虽会有所牺牲，但教学效果其实更加深远。

司法信息安全专业的实训平台的搭建上，可以在前期采用自行搭建平台的方式，在后期逐步引入厂商的网络安全训练平台和网络攻防竞赛平台，使用完整的“学练考评”平台，平台下一站式管理，课程全面、技术先进，同样的硬件资源可以支撑更多的学员练习、培训，界面简洁、免环境配置，学习体验感良好。形成良好的网络安全人才培养实训环境，为司法行政系统输送更多的网络安全专业人才。

参考文献

[1]张伟,李明.基于 VMware 的网络安全虚拟实验平台构建[J].实验技术与管理,2020,37(8):120-124

[2]教育部高等学校信息安全专业教学指导委员会.信息安全专业规范（第 2 版）[M].北京:高等教育出版社,2019.

[3]邓国斌,黎斌,沈萍高职网络信息安全专业人才培养实践与探索《福建电脑期刊》2020.12

[4]董玮《信息安全概论》课程思政教学实践探索《电脑知识与技术期刊》2021.11

作者简介：冯平（1980.2—），性别：男，民族：汉，籍贯：湖北武汉，学历：研究生，职称：（现目前的职称）讲师，研究方向：网络安全、大数据。