中国蓝盾
BLUEDON OF CHINA

蓝盾信息平安实验室建设方案

2010 年 05 月

蓝盾信息平安技术股份

目　录

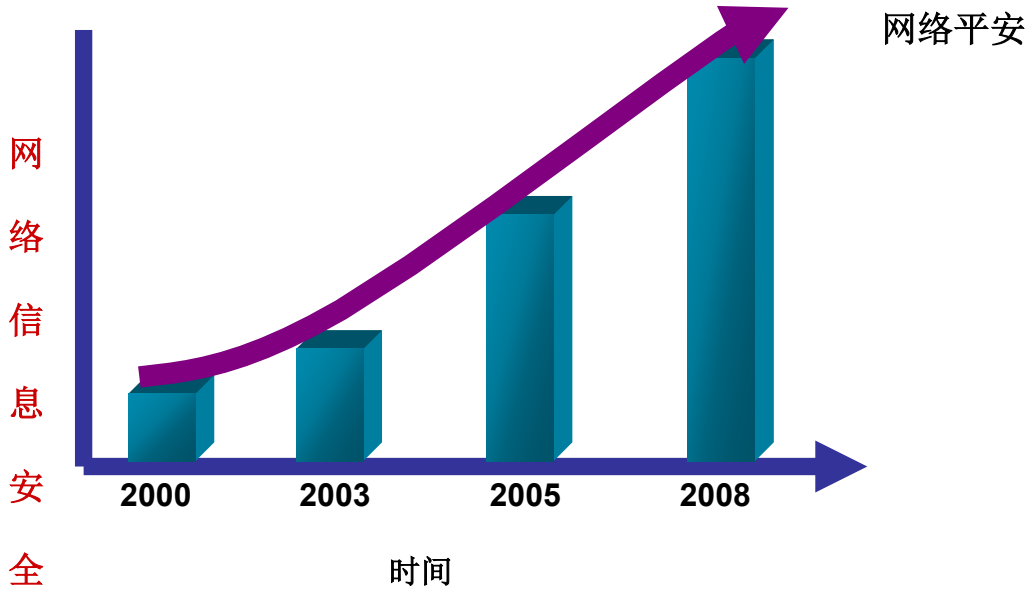
一、 概述

在过去的一段时间，教育领域以教育体制改革为核心，进行了院校合并、专升本、学员扩招、新校区建设等等变革，实现了教育行业规模的扩大，根本解决了社会对高学历人才的供需矛盾，建立了院校自我积累、自我开展的健康开展机制。

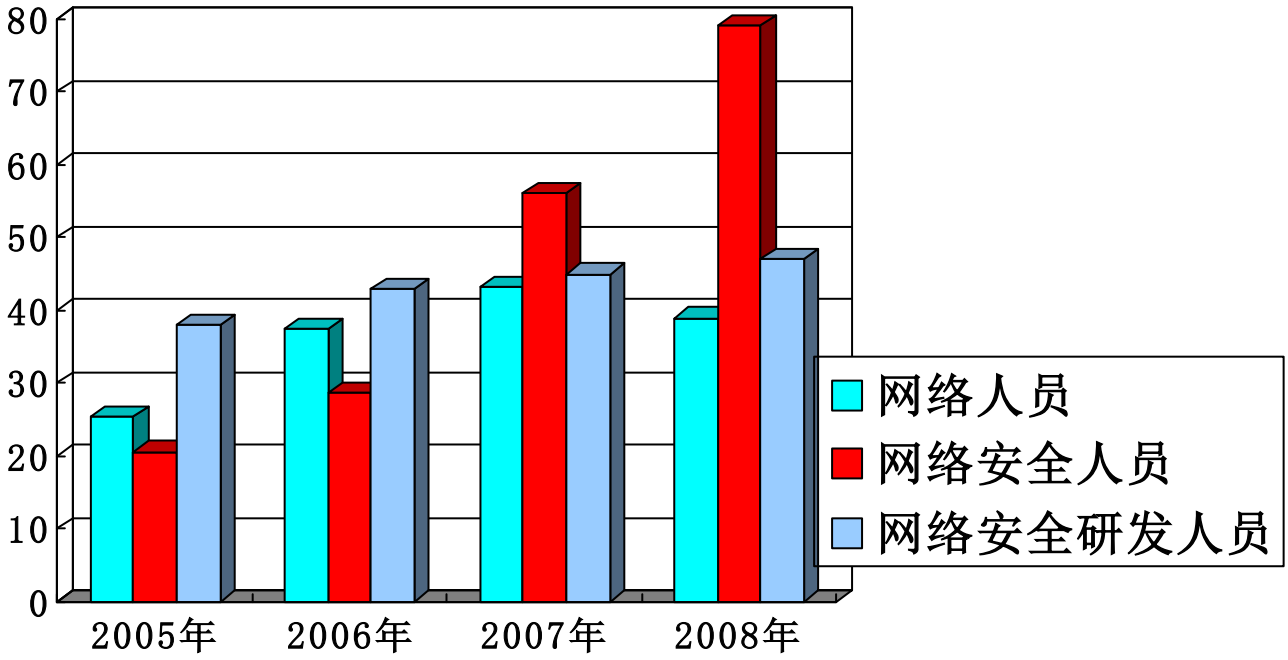
另一方面，随着我国信息化进程的不断推进，信息平安成为政府和企业广泛关注的焦点的问题。截至 2008 年 6 月，我国互联网用户已经从 2001 年的 2650 万激增到目前的 2.98 亿。随着互联网的开展，宽带使用者不断增加，种种网络病毒、网络犯罪也伴随而来，对企业和个人造成的影响和损失越来越明显。据有关报道显示，网络平安问题有 90％多是由于人的因素所引起的，防卫的松散、专业水平欠缺等问题普遍存在。在当前大量病毒爆发和黑客入侵导致网络威胁越来越多的严峻形势下，许多企业和单位都急需专业信息平安人才，信息平安人才出现严重匮乏。

信息平安，重在人才。然而，我国的网络信息平安专业教育刚刚兴起，培养的专业人才远远不能满足社会需求。国内一些知名高校普遍没有设置该专业。中科院研究生院虽然设有网络信息平安的研究生专业，但研究生总人数不超过 60 名，且大局部人毕业后都选择出国，或者从事科研工作。由此，网络信息平安人才供不应求也就缺乏为奇了，以至于出现“做平安的很多，懂平安的却很少”的状况。校园网络信息平安实验室正是在这种背景下应运而生。它随着信息科学技术教育的开展而建立起来的，在教学和科研中的重要作用日益显现，是学校教学实验环节中最重要的组成局部之一。校园网络信息平安实验室的建设水平、教学科研水平不仅反映出学校的办学水平，而且对学生的学习、教师的教学也将产生巨大的影响。

信息市场高速增长



信息平安人才短缺



校园网络信息平安实验室建设需求

复合型人才培养：

现在很多学生都面临就业难的问题，统计显示 70%毕业生找工作难，而工作岗位却很多，这就说明很多毕业生和企业用人标准之间存在一定差距，很多用人单位更希望应聘者不仅具备较好的理论知识，更应具备较好的实践能力，乃至对相关行业有一定认识。这就说明掌握理论、实践能力、行业知识的复合型人才才能更具竞争优势，更能满足社会的需要。

新技术、新应用研究：

院校的重点工作之一是：积极争取承当国家重大科研任务，大力促进产学研有机结合，充分发挥高校应用研究重要方面军和科技成果转化生力军的作用，大力加强根底学科研究，重点开展交叉学科研究，支持前沿高技术研究。

行业信息技术开展研究：

一方面，在很多行业中 IT 部门缺乏独立开发的能力，需要在此方面专业的研究机构提供帮助；另一方面院校可以利用自身技术与设施的优势效劳于社会，形成科研成果的生产力转化。

校企合作，共建网络学院：

建设蓝盾信息平安实验室要有较高的起点和全局的规划，蓝盾信息平安实验室的最终目的是促进产学研一体化，促进科研成果的转化并最终成为生产力，开展技术研究，并满足学校教学的需要。

通过校企合作，共建网络学院或网络实训学校，使校企双方都可受益，实现共赢。

对于学校，填补了计算机网络实验教学方面的空白；极大改善计算机网络实验教学的条件；具备了跟踪先进网络和通信技术，开阔学生的思路和眼界，提高教学水平和教学质量；在计算机网络技术方向，为创新人才培养基地提供良好的教学与科研条件。

对于企业，利用院校每年向国家输送的大量高素质的毕业生，他们对企业的设备和技术有深刻的认识和了解，对企业在高校和各行各业扩大影响和提高知名度很有益处。

二、建设目标

通过网络平安实验室的建设以及培训，到达以下目标：

〔1〕提高学生的实际动手能力

网络平安实验室提供目前主流的平安设备，如防火墙、入侵检测系统、平安扫描系统、网络防病毒系统、数字认证系统等，可以根据教学要求进行网络平安实验，实验的内容应充分结合当前网络平安技术以及国内市场的典型应用，模拟真实环境。通过系统的、不同平台环境的攻防演练，具体了解各种攻击防范手段，熟练使用各种攻防工具，提高反黑客技术与实战能力。

〔2〕培养不同类型不同层次的网络平安人才

网络平安实验室的实验内容充分考虑到学生的专业以及今后的开展方向，建议为学生定制至少 3 个方向的实验内容：网管人员、网络平安技术支持人员、网络平安研发人员。网络实验室需根据三种不同的角色进行相应的实验内容，培养出不同类型不同层次的网络平安实用性人才。

〔3〕成为有特色的培训基地

建成的网络平安实验室既可以为全校师生提供实际动手能力的环境，也要有能力为社会提供培训环境。通过这种特色的教学、丰富的有针对性实验内容，缩短在校学习与社会工作之间的距离，让每一位学员都能在职场上给自己找到一个最准确的定位，实现培养实用性人才的目标。

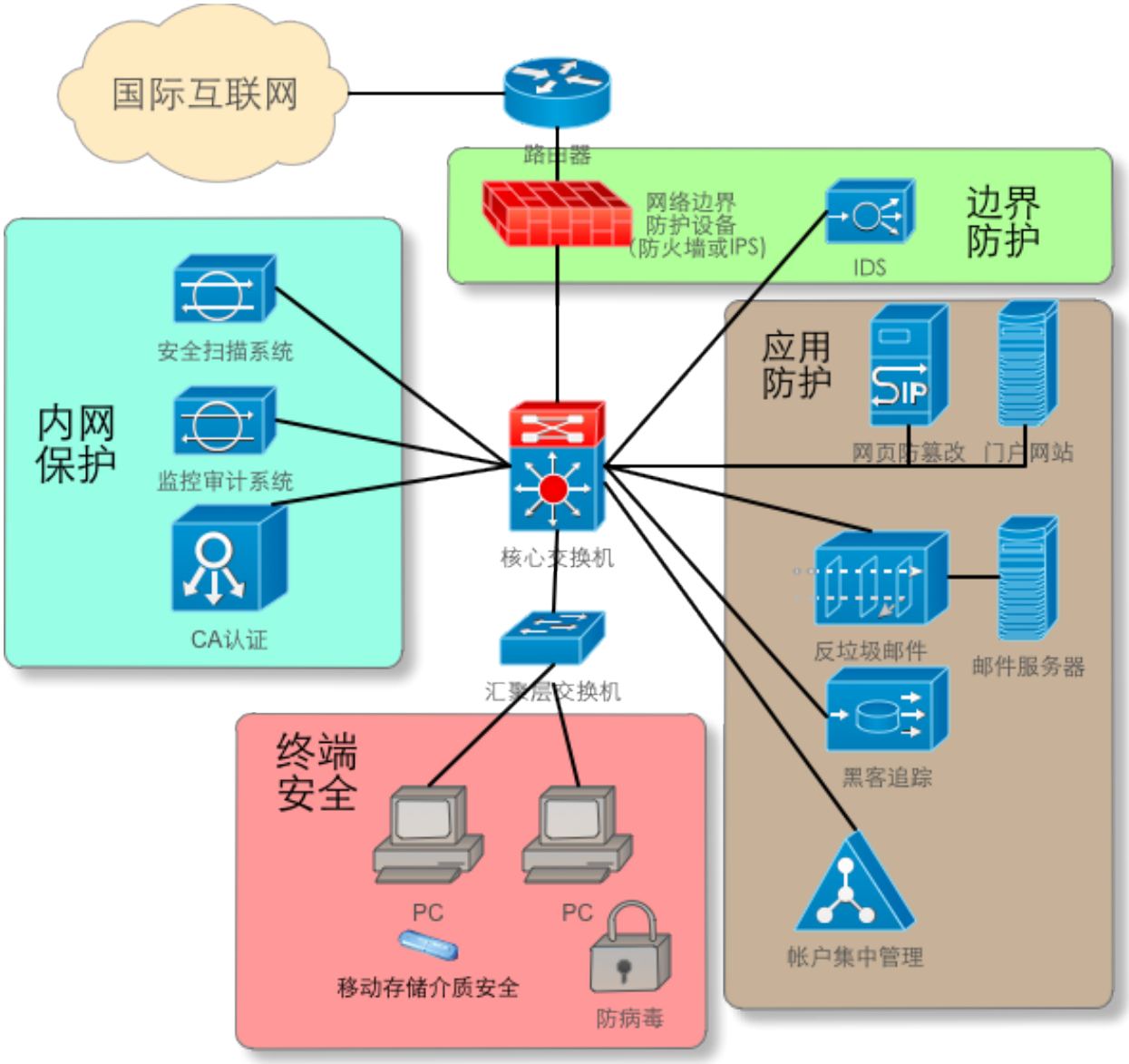
〔4〕丰富老师的知识面，提高在职老师的专业权威

由于网络平安实验室涵盖目前主流网络平安设备及技术，可以让老师系统的研究当前网络最前沿的技术动态和开展方向，并通过该实验室将理论和实践有机的结合起来，编写出一套新颖的教材，发表绝对权威的学术报告，在教育界网络平安领域树立专家形象。

三、蓝盾信息平安实验室解决方案

3.1 实验室网络结构图

信息平安实验室平台的支撑技术涉及到从根底设施技术、攻防关键技术、监控关键技术、重要应用关键技术以及信息平安效劳技术等所有信息平安保障体系的支撑技术。利用这些技术，该平台上集成了假设干个实验系统。该平台的构建技术表达了纵深综合防护机制，是一个多层次的、多维的大型信息平安系统，是一个学习、实验、实践以及科研的平台，具有较高集成度和较好可扩展性的多功能综合实验和测评效劳平台。其网络结构图设计如下：

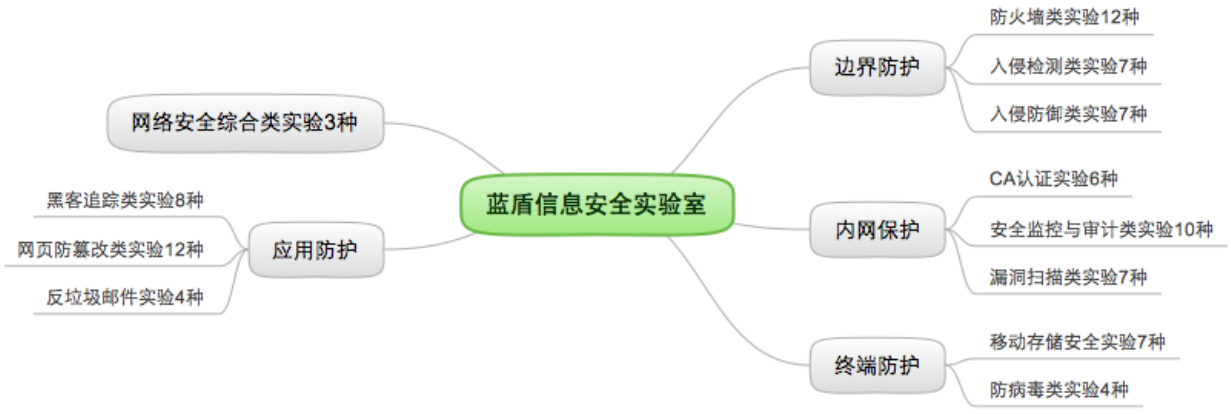


由上图可以看出：信息平安实验室里聚集了来自蓝盾信息平安技术股份的最新信息平安产品，以及当前常见的防病毒技术。实验室虚拟了中小企业典型信息平安部署的局域网，在整个网络拓扑中集成了防火墙、

入侵检测系统、平安扫描系统、网络防病毒系统、黑客侦查与追踪系统、内网平安保密系统等一系列信息平安产品。

信息平安实验室中设备一般采用集中部署。一组 4-6 件产品集中部署在一个机柜中，方便进行信息平安实验。

总体平安实验设备根据信息平安课程设置分成四大类：边界防护、内网保护、终端平安和应用防护。



3.2 方案设计特点

利用信息平安实验室的强大教学平台，蓝盾不仅提供自身相关的技术内容，还定期安排信息技术专家亲临信息平安实验室，为在校的大学生做面对面的现场指导。从而，为信息平安实验室搭建起一个厂商与成都电子高等专科学校间真正互通、互动的信息桥梁。方案设计特点如下：

3.2.1 标准化特点

信息平安实验室采用的蓝盾防火墙、蓝盾入侵检测系统、蓝盾平安扫描系统等系列产品符合国际标准，具备标准化原那么的特点，支持国际或国内通用标准的网络协议，如TCP/IP 协议等，而且还可以实现信息平安产品的联动技术，有效保证与其他网络之间的互连互通，具备代表性，符合高校统一施教的原那么。

先进性特点

信息平安实验室引进蓝盾信息平安技术股份的一系列信息平安产品，其技术紧跟国际水平，在国内属于领先地位，某些核心技术，如 DDoS 防御“零积累”技术、反向拍照技术等在国际上处于领先地位。

实用性特点

作为一个实践性很强的课程，信息平安实验是网络课程的重中之重。学生可以再实验室里进行防火墙技术实验、入侵检测技术实验、漏洞扫描技术实验、VPN 技术实验实验等覆盖范围广泛的综合信息平安实验，通过理论与实践相结合的培训模式，把网络的实际搭建能力和设备的调试能力列入了培训的关键环节，让学生真正掌握信息平安技术原理，具备规划、实施、管理大中型企业信息平安的能力，有利于学校培养实用性人才。

系统化特点

信息平安实验室不仅集中了常用的操作系统平台与各种应用效劳，而且聚集了当前常见的网络黑客攻击手段和较为全面的网络侦查专用设备，广泛覆盖了信息平安绝大多数领域，遵循了系统化建设的设计原那么。

灵活组合特点

实验室的信息平安设备能够灵活组合，具有多种配置方式，尽量模拟多种实际信息平安产品的典型部署方式。如蓝盾防火墙可以支持路由模式、透明模式、NAT 模式以及混合模式，入侵检测系统可以采用镜像口接入方式，也可以采用集线器〔HUB〕接入方式，平安扫描系统可以随时按需要移动接入到网络的各个节点，而且蓝盾系列产品都可以实现联动，可以模拟当前实际网络的多种典型部署方式。

可扩展性特点

本次模拟攻防实验室建设，在交换机、效劳器和 PC 机等网络设备中预留有足够的扩展空间，方便以后扩展。

3.3 实验内容列表

组建信息平安实验室的工作，可以按照实验室的性质和当前需要分为边界防护实验、内网保护实验、终端防护实验、应用防护实验和综合平安实验等几个方面。

序号	实验名称	掌握技能	面向对象	建议学时	难度
1	防火墙的典型安装与在网络中的部署	掌握防火墙根本配置与应用案例	中职、高职、本科	2	低
2	防火墙的初始设置		中职、高职、本科	2	低
3	防火墙路由规那么的设置		中职、高职、本科	4	中
4	防火墙工作方式的设置〔路由模式〕		中职、高职、本科	4	中
5	防火墙工作方式的设置〔NAT 模式〕		中职、高职、本科	4	中
6	防火墙工作方式的设置〔透明模式〕		中职、高职、本科	4	中
7	防火墙工作方式的设置〔混合模式〕		中职、高职、本科	4	中
8	防火墙平安规那么的设置		中职、高职、本科	4	中
9	DDoS 攻击模拟与 DDoS 防御		中职、高职、本科	4	中
10	地址绑定		高职、本科	4	中
11	连接速率设置		高职、本科	4	中
12	URL 过滤设置		高职、本科	4	中
13	链路负载设置		高职、本科	6	难
14	访问控制规那么设置		高职、本科	6	难
15	内容过滤设置		高职、本科	6	难
16	流量控制设置		高职、本科	6	难
17	防火墙日志记录分析		高职、本科	6	难
18	防火墙 VPN 模块典型安装与网络中部署方式	VPN 模块配置与应用案例	中职、高职、本科	2	低

19	防火墙 VPN 模块根本设置		中职、高职、本科	2	低
20	防火墙 VPN 模块 IPsec 通信		中职、高职、本科	4	中
21	防火墙 VPN 模块 L2TP 通信		中职、高职、本科	4	中
22	防火墙 VPN 模块 PPTP 通信		高职、本科	4	中
23	防火墙 VPN 模块集中管理		高职、本科	6	难
24	防火墙 VPN 模块隧道负载均衡		高职、本科	6	难
25	入侵检测系统的典型安装与在网络中的部署	掌握入侵检测系统根本配置与应用案例	中职、高职、本科	2	低
26	入侵检测系统的主要组成认识		中职、高职、本科	2	低
27	入侵检测系统的入侵信息的查看与分析		中职、高职、本科	4	中
28	自定义增参加侵特征模式		中职、高职、本科	4	中
29	入侵过程与常见的入侵手段		高职、本科	4	中
30	反向拍照技术追踪入侵攻击源		高职、本科	6	难
31	与防火墙如何进行联动设置实验		高职、本科	6	难
32	HTTP 协议的监控审计	掌握信息平安审计系统配置与应用案例	中职、高职、本科	2	低
33	FTP 协议的监控审计		中职、高职、本科	2	低
34	BT/电驴/迅雷等 P2P 传输工具监控审计		中职、高职、本科	4	中
35	QQ 协议的监控审计		高职、本科	4	中
36	MSN 协议的监控审计		高职、本科	6	难
37	社区/论坛的监控审计(QQ/天涯等)		高职、本科	6	难
38				2	低

	内网平安监控审计系统的典型安装与在网络中的部署	掌握内网平安监控审计系统根本配置与应用案例	中职、高职、本科		
39	共享文件/文件夹的平安规那么设置防护		中职、高职、本科	2	低
40	注册表规那么设置		中职、高职、本科	2	低
41	各种操作系统、应用程序审计日志的查看与分析		中职、高职、本科	2	低
42	设备管理和认证的设置		中职、高职、本科	4	中
43	外联监控功能		中职、高职、本科	4	中
44	主机资源审计功能		高职、本科	4	中
45	补丁管理与分发功能		高职、本科	4	中
46	文件加密、解密功能		高职、本科	6	难
47	与防火墙进行联动设置实验		高职、本科	6	难
48	漏洞扫描系统的典型安装与在网络中的部署	掌握漏洞扫描系统根本配置与应用案例	中职、高职、本科	2	低
49	漏洞产生的原因以及解决方法		中职、高职、本科	2	低
50	漏洞扫描结果的查看与分析		中职、高职、本科	4	中
51	漏洞扫描系统的根本功能		中职、高职、本科	4	中
52	对网络进行平安评估效劳		高职、本科	4	中
53	利用平安扫描系统进行模拟攻击测试		高职、本科	6	难
54	与防火墙如何进行联动设置实验		高职、本科	6	难
55	黑客侦查与追踪系统〔BD-IRS〕的典型安装与部署	掌握黑客追踪系统根本配置与应用案例	中职、高职、本科	2	低

56				4	中

	现代计算机犯罪的特点与主要技术手段		中职、高职、本科		
57	利用 BD-IRS 自动/手动方式获取目标主机与攻击行为相关的信息		中职、高职、本科	4	中
58	利用 BD-IRS 获取目标主机的应用效劳日志信息		高职、本科	4	中
59	蜜罐〔虚拟效劳〕实验		高职、本科	6	难
60	投放追踪探头，对攻击源进行查找		高职、本科	6	难
61	增加木马库的木马信息		高职、本科	6	难
62	增加操作系统文件信息库信息		高职、本科	6	难
63	用户管理	掌握账号集中管理与审计根本配置与应用案例	中职、高职、本科	2	低
64	访问控制		中职、高职、本科	4	中
65	Web 界面的实时监控用户操作行为		中职、高职、本科	4	中
66	关联分析用户在多台设备之间跳转操作		高职、本科	4	中
67	用户 Su 操作记录		高职、本科	4	中
68	明文传输〔telnet〕加密传输〔SSH〕的操作记录；		高职、本科	6	难
69	各种交互式命令〔sql 等〕操作		高职、本科	6	难
70	信息监控	掌握效劳器监控管理系统根本配置与应用案例	中职、高职、本科	2	低
71	网站管理		中职、高职、本科	4	中
72	效劳器的配置管理		中职、高职、本科	4	中
73	效劳器系统信息查看		高职、本科	4	中
74	平安管理		高职、本科	6	难

75	分级管理		高职、本科	6	难

76	前端日志收集		高职、本科	6	难
77	网站分类		高职、本科	6	难
78	网络防病毒软件的典型安装与部署	掌握防病毒系统根本配置与应用案例	中职、高职、本科	2	低
79	计算机病毒		中职、高职、本科	4	中
80	典型病毒分析与防范		中职、高职、本科	4	中
81	反病毒技术及病毒防范实验		高职、本科	6	难
82	如何从全网纵深防御角度考虑网络平安产品的选择与部署		高职、本科	6	难
83	防火墙与入侵检测系统的联动		高职、本科	6	难
84	内网平安保密及审计系统与防火墙、入侵检测系统之间联动的设置		高职、本科	6	难

3.4 实验进度设计

由于实验内容分为多个子系统进行，考虑到学生的学习知识需要遵循“循序渐进”规那么，故在设计该实验室时，我们对实验进度做如下设计：

第一阶段：根底理论与实验

根底理论：包括实验相关的根底理论、原型，实验原理以及测试原理等；

根底实验：主要是针对根底理论设计的相关实验。

第二阶段：子系统级功能演示与实验

子系统级功能演示：在经过第一阶段根底理论认识后，进入第二阶段各项子系统功能演示与实验，配套的文档资料包括：

(1) 内部存档资料：包括需求分析、概要设计、详细设计、测试等各阶段的技术文档；

(2) 面向学生文档：包括技术白皮书、用户使用说明书。

子系统级教学实验：借助于子系统的功能设计的教学实验，目的是让学生掌握系统功能，并通过教学实验对这些功能进行验证。

第三阶段：综合系统级功能演示与实验

综合系统级功能演示：在第二个阶段根底上，利用各子系统自身特点，实现多个子系统功能的有机结合、联动。

综合系统级实验：借助于综合系统级功能演示设计的教学实验，目的是让学生通过培训，对系统各项功能进行了解。

教学实验局部配套的文档资料要求：

(1) 实验指导书：实验题目、实验环境、实验目的、实验内容、实验要求、考前须知、实验报告要求；

(2) 实验教师参考书：实验目的、实验内容、实验要求、实验考前须知、实验步骤及流程、实验设计、实验测试、实验结果分析。

培训实验局部配套的文档资料要求：

学生培训教材：培训方案、培训教程、操作手册；

3.4.1 防火墙技术实验

配置一台蓝盾防火墙智能实验型〔BDFWH-EDU3030-SY〕，每组的学生实验用机都安装蓝盾防火墙管理软件，学生也可以通过 GUI 管理方式连接到防火墙上进行相关内容实际操作学习。

该实验主要是让学生充分了解防火墙技术原理，熟悉和配置防火墙。在这个网络实验环境中，学生可以掌握以下防火墙主要技术：

- 防火墙的典型安装与在网络中的部署
- 防火墙路由规那么的设置
- 防火墙工作方式的设置〔路由、NAT、透明、混合〕
- 地址转换〔NAT〕
- 防火墙平安规那么的设置
- DDoS 攻击模拟与蓝盾 DDoS 防御实验
- 各种访问控制的规那么设置
- 内容过滤技术
- 效劳器监控分析技术
- 即时监控软件控制设置
- 流量控制等设置
- 入侵检测功能
- 防火墙日志记录分析
- VPN 功能

- 其他

3.4.2 VPN 技术实验

配置的蓝盾防火墙智能实验型〔BDFWH-EDU3030-SY〕 自带有 VPN 模块，可以作为 VPN 网关使用。每组的学生实验用机都安装蓝盾 VPN 客户端软件以及蓝盾智能证书模块〔USBKEY〕，而且在实验室网络中特别使用一台 PC 机拨号上网〔或者 ADSL 上网〕，安装蓝盾 VPN 客户端软件以及蓝盾智能证书模块〔USBKEY〕，作为移动 VPN 实验使用。

该实验主要是让学生充分了解 VPN 技术原理，熟悉和配置常见的 VPN 网关。在这个网络实验环境中，可以进行相互之间网关对网关型的 VPN 连接实验，还有网关对移动 VPN 型的实验。

学生可以掌握以下防火墙主要技术：

- VPN 网关的典型安装与在网络中的部署
- VPN 技术原理
- VPN 根本功能
- VPN 的平安机制
- 其他

3.4.3 入侵检测技术实验

在网络忠配置一台蓝盾入侵检测系统〔BD-NIDS-EDU5050-SY〕，学生实验用机都安装蓝盾入侵检测系统控制中心软件，学生也可以通过 GUI 管理方式连接到蓝盾入侵检测系统上进行相关内容实际操作学习。

该实验主要是让学生充分了解入侵检测技术原理，熟悉和配置常见的入侵检测系统。

学生可以掌握以下入侵检测主要技术：

- 入侵检测系统的典型安装与在网络中的部署
- 入侵检测系统的主要组成认识
- 入侵检测系统的入侵信息的查看与分析
- 自定义增参加侵特征模式
- 入侵过程与常见的入侵手段
- 反向拍照技术追踪入侵攻击源
- 与蓝盾防火墙如何进行联动设置实验
- 其他

3.4.4 漏洞扫描技术实验

在网络中配置一台蓝盾平安扫描系统〔BD-SCANNER-EDU5050-SY〕，学生实验用机都安装蓝盾平安扫描系统控制中心软件，学生也可以通过 GUI 管理方式连接到蓝盾平安扫描系统上进行相关内容实际操作学习。

该实验主要是让学生充分了解漏洞到描技术原理，熟悉和配置常见的漏洞扫描系统。

学生可以掌握以下漏洞扫描主要技术：

- 平安扫描系统的典型安装与在网络中的部署
- 漏洞产生的原因以及解决方法
- 平安扫描结果的查看与分析
- 平安扫描系统的根本功能
- 如何对网络进行平安评估效劳
- 如何利用蓝盾平安扫描系统进行模拟攻击测试
- 与蓝盾防火墙如何进行联动设置实验
- 其他

3.4.5 内网平安保密及审计技术实验

实验室配置一台蓝盾内网平安保密及审计系统〔BD-SECSYS-EDU5050-SY〕，蓝盾内网平安保密及审计系统主要包括三局部组件：网络平安监控器(BD-SECSYS-N)、主机代理(BD-SECSYS-H)和控制中心(BD-SECSYS-C)。网络平安监控器采用专用硬件设备以旁路方式接入内网关键点，主机代理以效劳的方式运行在内网被保护主机上，控制中心提供显示和管理配置功能。网络平安监控器部署在网络出口的交换机上，学生实验用机都安装蓝盾内网平安及审计系统的主机代理客户端软件和控制中心软件，学生可以通过 GUI 管理方式连接到蓝盾内网平安保密及审计系统上进行相关内容实际操作学习。

该实验主要是通过对蓝盾内网平安保密及审计系统的讲解和操作，让学生充分了解内网平安保密及审计技术原理，熟悉和配置常见的平安审计及保密系统。

学生可以掌握以下平安审计及保密主要技术：

- 蓝盾内网平安保密及审计系统的典型安装与在网络中的部署
- 共享文件/文件夹的平安规那么设置防护
- 注册表规那么设置
- 各种操作系统、应用程序审计日志的查看与分析
- 设备管理和认证的设置
- 如何使用外联监控功能

- 如何使用主机资源审计功能
- 如何使用补丁管理与分发功能
- 如何使用文件加密、解密功能
- 与蓝盾防火墙如何进行联动设置实验
- 其他

3.4.6 黑客侦查与追踪技术实验

实验室配置一套蓝盾黑客侦查与追踪系统〔BD-IRS-EDU〕，BD-IRS-EDU 是专门针对计算机信息犯罪而开发的一种快速、准确、可靠的辅助技术侦察手段。 该实验主要是通过对蓝盾黑客侦查与追踪系统〔BD-IRS-EDU〕的讲解和操作，让学生充分了解现代计算机犯罪的特点与主要技术手段，了解攻防技术原理。

学生可以掌握以下主要技术：

- 蓝盾黑客侦查与追踪系统〔BD-IRS-EDU〕的典型安装与部署
- 现代计算机犯罪的特点与主要技术手段
- 利用 BD-IRS-EDU 自动/手动方式获取目标主机与攻击行为相关的信息
- 利用 BD-IRS-EDU 获取目标主机的应用效劳日志信息
- 蜜罐〔虚拟效劳〕实验
- 投放追踪探头，对攻击源进行查找
- 熟悉增加木马库的木马信息
- 熟悉增加操作系统文件信息库信息
- 其他

3.4.7 防病毒技术实验

实验室配置一套诺顿网络版防病毒软件，在网络中配置了一台诺顿网络版效劳器，学生实验用机上安装防病毒客户端软件。 该实验主要是让学生充分了解计算机病毒原理及防范技术。

学生可以掌握以下主要技术：

- 网络防病毒软件的典型安装与部署
- 计算机病毒知识
- 典型病毒分析与防范
- 反病毒技术及病毒防范实验
- 其他

3.4.8 数字认证技术实验

实验室配置一台 CA 数字证书效劳器。 该实验主要是让学生充分了解数字认证技术。

学生可以掌握以下主要技术：

- CA 认证效劳器的典型安装与部署
- PKI 知识与数字签名技术原理
- 数字证书的常见应用与功能介绍
- 数字证书的类型与数字证书的管理
- CA 工作原理
- 证书的使用流程
- 其他

3.4.9 网络平安综合实验

我们提供的网络平安实验室方案是基于 MPDRR 模型〔M-management，P-protect，D-detection，R1-responce，R2-recovery〕模型构建的，符合网络平安系统整体性和动态性的特点。将多种网络平安技术和优秀网络平安产品在技术上有机集成，实现平安产品之间的互通与联动，是一个统一的、可扩展的平安体系平台。

在对以上各个子系统〔防火墙、入侵检测、漏洞扫描等子系统〕的深入了解和有较好的操作水平的根底上，利用各子系统自身特点，实现多个子系统功能的有机结合、联动，进行网络平安综合实验，主要是让学生认识到网络平安系统是整体的、动态的。因此，要真正实现一个系统的平安，就需要建立一个从保护、检测、响应到恢复的一套全方位的平安保障体系。

学生可以掌握以下主要技术：

- 如何从全网纵深防御角度考虑网络平安产品的选择与部署
- 防火墙与入侵检测系统的联动
- 内网平安保密及审计系统与防火墙、入侵检测系统之间联动的设置
- 其他

3.4.10 攻防演练实验

实验室集中了当前常见的黑客攻击手段和较为全面的网络平安设备〔蓝盾防火墙、蓝盾扫描器、蓝盾黑客侦查与追踪系统、蓝盾内网平安保密及审计系统等〕，通过系统的、不同平台环境的攻防演练，具体了解各种攻击防范手段，熟练使用各种侦查工具，提高反黑客技术与实战能力。

四、信息平安实验室课程建设体系

4.1 课程介绍

本课程主要针对校企合作院校，信息平安专业和计算机网络、应用专业信息平安方向的高校学生，实验配有全套的蓝盾网络平安实验设备，现场构建真实的交互实验环境，使学生能够亲自动手操作防火墙、平安审计、漏洞扫描等系列产品。结合完整的技术手册和产品说明书，实习指导书，通过讲授、实验和问题解答的模式，为学生获取珍贵的设备操作经验。使学生具有专业的技术操作，出色的问题解决能力，保证学生对学习内容的充分理解、融会贯穿。

课程教学采用蓝盾公司先进的〔数字化学习、电子化学习、网络化学习〕教学系统并辅以动手实验，整个实验室分 4 个层次进行的教育方案，教材采用蓝盾内部、推荐教材、联合编著教材融合到校内选定教材的方式进行教学。并根据学校教学进程安排，把 100 多个实验分布到每个学期当中完成。

4.2 信息平安实验室理论课程安排

学期	增加开设课程	学时	推荐教材	备注
第二学期	信息平安法律法规	32	《信息平安标准与法律法规》武汉大学出版社　　陈忠文 《信息平安法律法规与管理》重庆大学出版社　　戴宗坤	二选一
	网络与信息平安技术	64	《网络与信息平安技术》哈尔滨工业大学出版社　　霍成义　卢宏才	理论+实践
	信息防火墙	42	文件夹的加密、解密、伪装；数据的恢复，磁盘的诊断；即时通讯与 WEB 聊天室的应用；邮件效劳器的架构与应用；	蓝盾内部教材一体化
	移动平安存储技术	36	信息平安实验室	蓝盾内部教材一体化
第三学期	平安扫描技术	36	信息平安实验室	实践
	黑客追踪技术	36	信息平安实验室	实践
	效劳器架构与管理	40	效劳器的架构技术	

			效劳器的监控与管理技术 网络优化与局域网渗透技术	蓝盾内部教材一体化
	PKI 技术	80	《PKI 原理与技术》 电子科技大学出版社　　佘堃 / 郑方伟	理论+教学
	《VPN 技术》	64	《VPN 技术》 机械工业出版社　　高海英	理论+实践
第四学期	防火墙技术	64	《防火墙原理与技术》	理论+实践
	入侵检测技术	64	《入侵检测技术》 高等教育出版社　　李剑	理论+实践
	Web 应用平安与攻击技术	64	《黑客大曝光：Web 应用平安机密与解决方案》 电子工业出版社　王炜,文苗罗代升译	理论+ 实践
	信息平安审计	32	信息平安实验室	实践
	内网平安审计	32	信息平安实验室	实践
	防病毒技术	25	信息平安实验室	实践
	网络隔离技术	64	《网络隔离与网闸》 机械工业出版社　　万平国	理论教学
第五学期	ISEC-1201	20	《平安根底》	综合培训
	ISEC-1202	20	《用网平安》	综合培训
	ISEC-2201	20	《信息平安根底》	综合培训
	ISEC-2202	25	《操作系统平安》	综合培训
	信息平安综合实训	2 周	企业案例+实验室平台	工程
	等保和风险评估	24	工程方式教学	案例
	素质训练	16	专业工程师/专家指导	情景式

4.3 信息平安实验室实践课程安排

课程代码	课程	教学内容	教学方法

1	防火墙技术	防火墙的根本配置、防火墙工作方式设置，访问控制设置、流量控制设置、平安规那么设置，地址绑定、链路负载设置、内容过滤设置。	教学、实验
2	入侵检测技术	入侵检测系统的分类、部署，入侵信息查看与分析、反向拍照技术、入侵过程与常见入侵手段、自定义增参加侵特征模式，几种主流的入侵检测方式。	教学、实验
3	工程实战一	入侵检测系统与防火墙的联动实训	案例
4	内网平安审计	各种操作系统应用程序审计日志的查看与分析、主机资源审计、文件加密与解密的功能，设备管理和认证的设置，补丁管理与分发功能。	教学、实验
5	平安扫描技术	平安扫描的典型安装与部署，漏洞产生的原因及解决方法，扫描的分析，网络平安的评估，模拟攻击测试。	教学、实验
6	CA 认证技术	CA 认证效劳器的典型安装与部署，PKI 知识与数字签名技术应用，数字证书的功能和管理，CA 工作原理、数字证书使用流程。	教学、实验
7	工程实战二	❶内网审计技术、平安扫描系统同防火墙的联动实训 ❷利用淘宝网〔其它电子商务网站〕通过 CA 认证技术实现网上交易的平安实训	教学、实验
8	黑客追踪技术	利用手动/自动方式获取目标主机信息、应用效劳日志信息，投放追踪探头，查找攻击源，增加木马库木马信息、增加操作系统文件信息库信息。	教学、实验
9	工程实战三	密罐实验 QQ 聊天记录跟踪 全程追踪入侵 JSP 网站效劳器	案例教学
10	反垃圾邮件技术	过滤功能模块、管理功能模块、日志接收功能模块、日志分析功能模块	教学、实验

11	网页防篡改技术	实时报警与恢复、自动发布功能，平安通道，支持多虚拟主机、目录，支持动态网页，权限、策略管理，查询审计，效劳器联动功能。	教学、实验
12	工程实战四	利用僵尸网络控制用户 PC 发送垃圾邮件 利用花生壳技术发送垃圾邮件	模拟公司
13	移动平安存储技术	移动数据生命周期防护、多层次的数据平安机制，在线/离线策略支持，移动介质的病毒免疫，数据自锁。	教学、实验
14	防病毒技术	防病毒软件的安装与部署，典型病毒的分析与防范，如何从全网纵深防御角度考虑网络平安产品的选择和部署。	教学、实验
15	攻击技术	攻击工具的应用，如何攻击 WEB 应用程序，踩点和扫描；如何攻击 WEB 平台，攻击 WEB 认证/授权，SQL 注入和数据存储攻击，DOS 拒绝效劳攻击，平安扫描器的应用；WEB 效劳器攻击，现实世界中的 XSS 攻击。	教学、实验
15	风险评估	风险评估的扫描工具，手工评估思想与评估方法，平安管理策略的自动化评估系统。	教学、实验、模拟公司
16	素质训练	信息平安规那么与标准：IT 职业规划、沟通技巧、团队合作、专业技术标准、面试技巧等职业技能培训。	工程师/专家指导
应用密码学实验工程			
实验工程			
17	1. 对称密码-DES 单步加密实验 2. 对称密码-DES 算法实验 3. 对称密码-3DES 算法实验		实验 注：提供源码

	4. 对称密码-AES 算法实验 5. HASH 算法-MD5 算法实验 6. HASH 算法-SHA-1 算法实验 7. 非对称密码-RSA 算法实验 8. 非对称密码-DSA 数字签名实验	
18	1. 古典密码算法实验 2. 对称密码-DES 算法实验 3. 对称密码-IDEA 算法实验 4. 对称密码-RC4 算法实验 5. 对称密码-AES 算法实验 6. 非对称密码-RSA 算法实验 7. 非对称密码-ECC 算法实验 8. HASH 算法-MD5 算法实验 9. 非对称密码- RSA 数字签名实验	实验 注：提供源码和函数接口

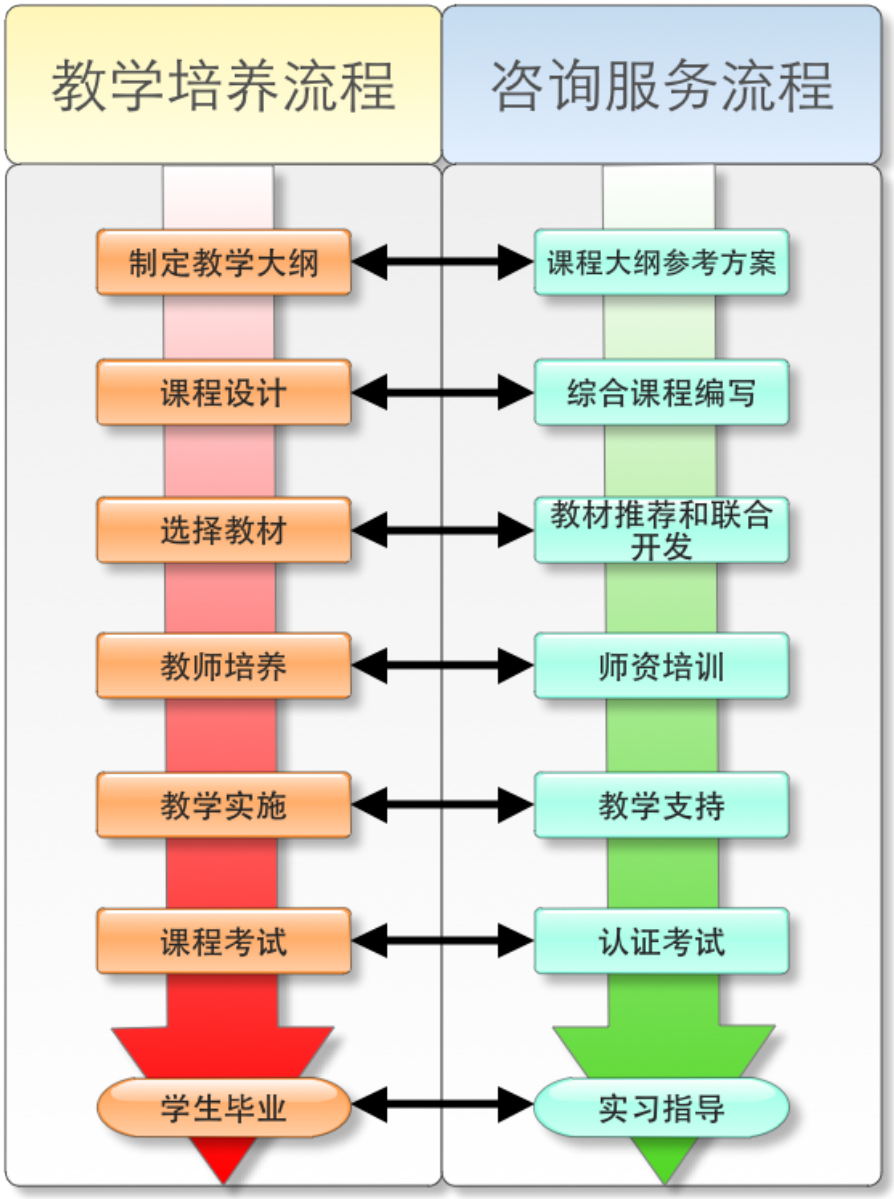
4.4 信息平安实验室师资培养

蓝盾师资培养课程体系	考核方式	培养目标	考核说明
蓝盾认证专业讲师培养 ▸网络知识、信息平安知识培训 ▸实验操作、授课技巧培训 ▸蓝盾产品、综合案例培训	实时考核	BDPI 蓝盾专业讲师	试讲考核 理论考核 调试考核 实验考核
蓝盾认证金牌讲师培养 ▸信息平安技术攻关培训 ▸信息系统平安解决方案培训 ▸信息平安工程管理、监理培训 ▸信息平安工程开发培训	应用考核	BDGI 蓝盾金牌讲师	采用笔试考核 通过工程审核 完成工程评估
蓝盾认证高级讲师培养 ▸信息平安技术改造、技术革新培训 ▸信息平安规划、诊断管理培训 ▸信息平安领域专家培训	综合考核	BDSI 蓝盾高级讲师	专业课题研究 技术论文发表

蓝盾实验室助理教师培训			
▸交换机、路由器技术理论知识 ▸防火墙、IDS、VPN 根底理论知识 ▸网络平安协议根底理论知识 ▸ 网络攻防技术根底理论知识 ▸计算机根底的根本操作 ▸计算机操作系统的应用和管理 ▸交换机、路由器的根本配置 ▸ 防火墙、IDS、VPN 根本配置 ▸ 网络攻防的根本技术 ▸ 实验室的管理技术	技术考核	BDAT 蓝盾助理教师	采用试验方式 进行阶段考试

五、蓝盾信息平安专业教学咨询效劳

作为业界专注于信息平安的咨询效劳商，蓝盾提供最全面针对高等学校信息平安专业方向的教学咨询效劳。根据蓝盾对于信息平安市场的深入了解和长期研究，信息平安实验室建设不仅仅表达在教学设备采购上，更表达在与教学培养流程相适应的咨询效劳流程上。从学校教学流程的第一步就要开始提供与之相适应的咨询效劳。因此，蓝盾针对教学培养流程的每个环节为客户成都电子高等专科学校提供最贴心的教学咨询支持。



教学培养与咨询效劳关联图