高校信息安全人才培养

铱迅信息 杨谦

南京铱迅信息技术股份有限公司

目录

BACKGROUND

信息安全人才培养背景

信息安全人才培养背景

中央网信办高度重视

今日头条 首页 / 新闻 / 正文

2

微博

Qzone

微信

中央网信办等下文：支持高校开设网络安全“特长班”

微言教育 2016-07-08 15:16

中央网络安全和信息化领导小组办公室、国家发改委、教育部等六部门近日联合印发《关于加强网络安全学科建设和人才培养的意见》，提出要加快网络安全学科 专业和院系建设，有条件的高校可通过整合、新建等方式建立网络安全学院；要创新网络安全人才培养机制，鼓励高校适度增加相关专业推荐优秀应届本科毕业生免 试攻读研究生名额；要强化网络安全师资队伍建设，聘请经验丰富的网络安全技术和管理专家、民间特殊人才担任兼职教师等。更多内容请看下文。

【加快网络安全学科专业和院系建设】

《意见》提出，在已设立网络空间安全一级学科的基础上，加强学科专业建设。发挥学科引领和带动作用，加大经费投入，开展高水平科学研究，加强实验室等建 设，完善本专科、研究生教育和在职培训网络安全人才培养体系。有条件的高等院校可通过整合、新建等方式建立网络安全学院。通过国家政策引导，发挥各方面积 极性，利用好国内外资源，聘请优秀教师，吸收优秀学生，下大功夫、大本钱创建世界一流网络安全学院。

http://www.toutiao.com/i6304849503455281665/

信息安全人才培养背景

加快网络安全学科专业和院系建设
创新网络安全人才培养机制
加强网络安全教材建设
强化网络安全师资队伍建设
推动高等院校与行业企业合作育人、协同创新
加强网络安全从业人员在职培训
加强全民网络安全意识与技能培养
完善网络安全人才培养配套措施

信息安全人才培养背景

相关数据显示：近年来，我国高校学历教育培养的信息安全专业人才仅3万余人，而总需求量超过70万人，人才缺口高达95%

中国青年网 youth.cn 首页 >> 教育资讯 >> 教育新闻 >> 正文

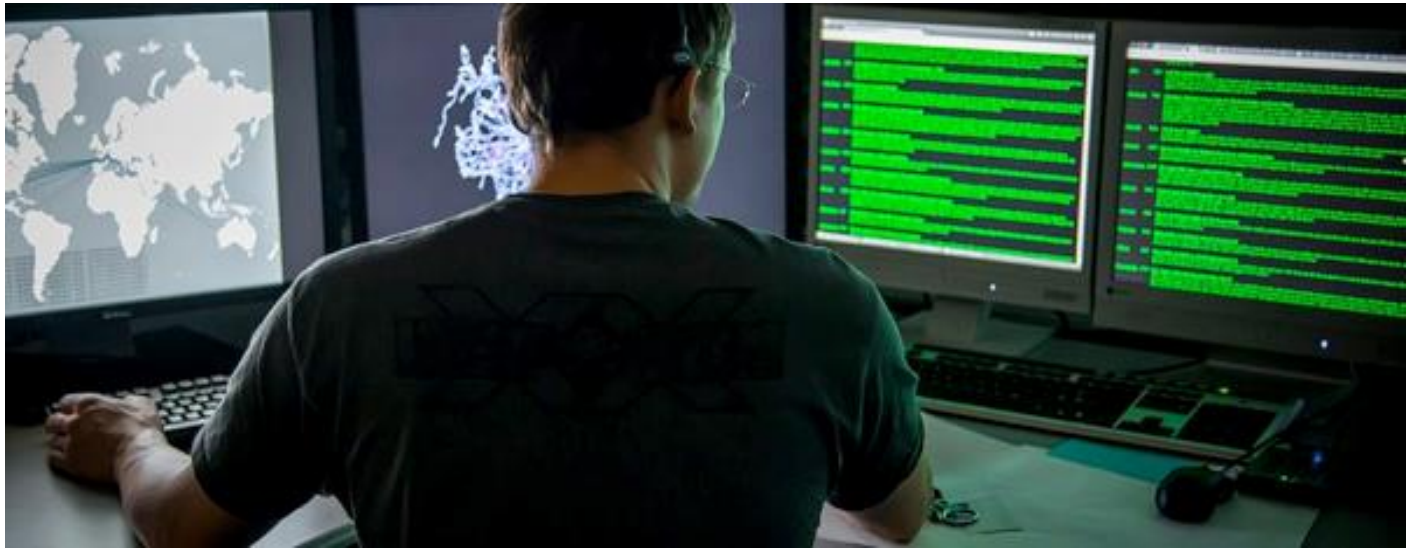
供需缺口高达95% 高校网络安全人才培养亟需重视

发稿时间：2016-11-30 08:37:00　　来源：　中国新闻网　　中国青年网

21世纪什么最重要？是人才！相关数据显示：近年来，我国高校学历教育培养的信息安全专业人才仅3万余人，而总需求量超过70万人，人才缺口高达95%。市场上各大公司求贤若渴，网络安全人才的培养已迫在眉睫。

由于网络安全行业非常强调动手能力，讲究人与人的技术对抗，大学校园内往往不具备这样的机会与条件，难以培养出具备实战对抗能力的安全人才。很多名校毕业的学生在进入工作岗位后，往往不及一些没有正式学历的员工，很多知识都要从头学起。据估算，1个网络安全人才培养成本约为46万美金，这样高的成本也阻碍了人才培养的数量。

SOC安全分析师技能要求



计算机基础知识：网络、操作系统、数据库、应用软件、程序代码、 TCP/IP …大学学习

安全产品知识：防火墙、DOS防护、入侵防御、数据库审计、web应用防火墙、漏洞扫描、堡垒机、VPN、防病毒软件、邮件网关、终端管理软件、PKI……

安全运维知识：风险管理、安全域边界防御、网络准入、服务器管理、安全配置加固、应用开发安全管理、终端管理、BYOD管理、虚拟化数据中心管理……

黑客入侵知识：踩点、扫描、系统入侵、web入侵、木马后门、嗅探、劫持、密码破解、社会工程、清除痕迹

最新安全动态：流行的病毒、新发现的漏洞、流行的入侵手段、最新安全态势、紧急加固措施

安全分析技能：恶意代码逆向分析、软件漏洞挖掘、安全产品防护策略绕过，业务逻辑安全漏洞分析、通信协议漏洞分析、蜜网蜜罐、入侵取证、反向追溯

信息安全主管技能要求

计算机基础知识：网络、操作系统、数据库、应用软件、程序代码、TCP/IP……

安全产品知识：防火墙、DOS防护、入侵防御、数据库审计、web应用防火墙、漏洞扫描、堡垒机、VPN、防病毒软件、邮件网关、终端管理软件、PKI……

安全管理知识：安全策略、组织安全、人员安全、物理环境安全、访问控制、密码学、操作安全、通信安全、系统获取开发安全、安全事件管理……

安全标准政策：ISO27001、等级保护、ISO20000、PCI DSS、ITIL、各行业安全标准……

最新安全动态：安全合规政策要求、安全标准解析、安全产品、安全方案、新技术安全研讨、

安全最佳实践：IT安全风险管理实践、IT安全规划实践、信息安全管理制度、安全岗位控制指标实践、安全运维最佳实践、敏感信息保护实践

世界变化太快

- CCNP、RHCE、MCSE、DBA、VCP
- CISP、CISSP、CISA、CSSLP
- CEH、CHFI、LPT、ECSP、CWASP
- CRISC、ISO27001LA、ISO20000 LA
- CISM、CISTE、CCSK
- ITIL、BCCE、 COBIT 、CBCP

- Firebug、Fiddler、Wireshark、Tcpdump、burpsuite、sqlmap
- Python、jQuery、C、C++、C#、perl、php、java、asp、.net、
- MySQL、MSSQL、Oracel、Postgre、Access、SQLite、Hadoop
- OWASP、WASC、XSS、CSRF

- FW、IPS、IDS、WAF、AV、APT、HNS、Scanner、BVS、SOC、DBS、GAP、PKI、CA、ADS、WSM、AAS

- Nmap、Nessus、Superscan、SolarWinds、Cain&Abel、LOphtCrack、IDA Pro、ZAP、Metasploit、Havij、Snort、CANVAS、zoomeye、shodan
- Wooyun、freebuf、virustotal、ShellShock

METHODS

信息安全人才培养方法

CISP培训

CISP既“注册信息安全专业人员”，系国家对信息安全人员资质的最高认可。英文为Certified Information Security Professional （简称CISP），CISP系经中国信息安全测评中心实施国家认证。

1、CISE（注册信息安全工程师）：

适合政府、各大企事业单位、网络安全集成服务提供商的网络安全技术人员

2、CISO（注册信息安全管理人员）：

适合政府、各大企事业单位的网络安全管理人员，也适合网络安全集成服务提供商的网络安全顾问人员

3、CISA（注册信息安全审核员）：

适合政府、各大企事业单位的网络安全技术人员、也适合网络安全集成服务提供商的网络安全顾问人员

CISP培训

认证介绍

国家注册信息安全专业人员(简称：CISP）是有关信息安全企业，信息安全咨询服务机构、信息安全测评机构、社会各组织、团体、企事业有关信息系统（网络）建设、运行和应用管理的技术部门（含标准化部门）必备的专业岗位人员，其基本职能是对信息系统的安全提供技术保障，其所具备的专业资质和能力，系经中国信息安全测评中心实施注册。2014年3月，全国获得CISP认证资格人员已超过10000名。

认证机构

中国信息安全测评中心是我国专门从事信息技术安全测试和风险评估的权威职能机构。依据中央授权，开展信息安全服务和专业人员的能力评估与资质审核。测评中心自2002年开启“注册信息安全专业人员（CISP）”资格认证注册工作。天融信成为第一个经测评中心授权的“国家注册信息安全专业人员”认证培训机构。

认证价值

对组织的价值：

- 高素质的信息安全专业人才队伍，是信息安全的保障；
- 信息安全人员持证上岗，满足政策部门的合规性要求；
- 为组织实施信息安全岗位绩效考核提供了标准和依据；
- 是信息安全企业申请安全服务资质必备的条件。

对个人的价值：

- 适应市场中越来越热的对信息安全人才的需求；
- 通过专业培训和考试提高个人信息安全从业水平；
- 证明具备从事信息安全技术和管理工作的能力；
- 权威认证提升职场竞争中的自身优势；
- 可以获取信息安全专业人士的认可，方便交流。

认证分类

根据工作领域和实际岗位的需要，CISP分为两个基础类别：

注册信息安全工程师（CISE）	主要从事信息安全技术开发服务工程建设等工作。
注册信息安全管理员（CISO）	主要从事信息安全管理等相关工作

注册条件

CISP认证适合国家信息安全测评机构、信息安全咨询服务机构、社会各组织、团体、企事业单位从事信息安全服务或高级安全管理工作的人员。

注册人员需满足以下教育与工作经历

学历	工作经历
硕士研究生以上	1年工作经历
本科毕业	2年工作经历
大专毕业	4年工作经历

以上经历中至少包含1年从事信息安全相关工作。

知识体系

CISP的知识体系结构涵盖了信息安全的各个方面，共包括五个知识类，每个知识类根据其逻辑划分为多个知识体，每个知识体包含多个知识域，每个知识域由一个或多个知识子域组成。

关于考试

CISE和CISO注册证书持有人的工作岗位和工作领域的不同，考试的侧重点有所区别，所对应的试题比例也不同。（以CNITSEC公布资料为准）

知识类别 \ 资质类型	CISE	CISO
信息安全保障概述	10%	10%
信息安全技术	50%	30%
信息安全管理	20%	40%
信息安全工程	10%	10%
信息安全标准和法律法规	10%	10%

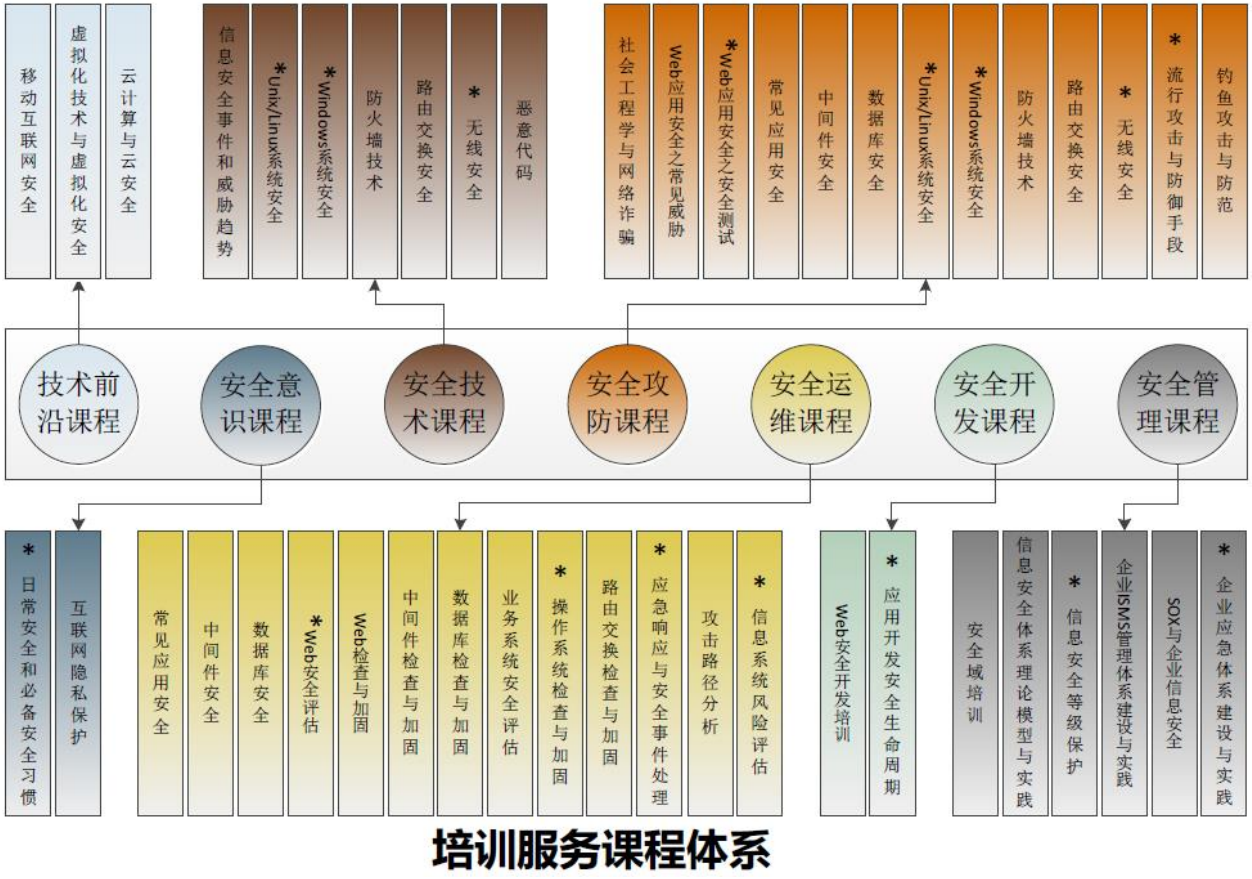
考试题型均为单项选择题，共100题，每题1分，得到70分以上（含70分）为通过。

关于培训

培训为脱产形式，上课时间 8天，期间安排休息一

时间	课程编码	课程名称	课时内容
第一天	CISP0101	信息安全保障基本知识/信息安全保障基本实践	信息安全保障基本知识
			信息安全保障原理
			典型信息系统安全保障模型与框架
			信息安全保障工作概况
			信息系统安全保障工作基本内容
	CISP0401	信息安全工程原理/信息安全实践	信息安全工程理论背景
			安全工程能力成熟度模型
			安全工程实施实践
			信息安全工程监理
第二天	CISP0201	密码学基础	密码学基础概念
			密码学算法（对称、非对称、哈希函数）
	CISP0202	密码学应用	VPN技术
			PKI/CA系统
第三天	CISP0203	访问控制与审计监控	访问控制模型
			访问控制技术
			审计和监控技术
	CISP0204	网络协议及网构安全/网络安全设备	TCP/IP协议安全
			无线安全/移动通信安全
			网络其构安全
			防火墙技术
			入侵检测技术
			其他网络安全技术
第四天	CISP0205	操作系统安全	操作系统基础/安全机制
			Unix安全实践
			Windows安全实践
	CISP0206	系统应用安全	数据库基础知识及安全机制/数据库管理
			web服务基础、web浏览器与服务安全
			电子邮件安全/FTP安全、常用软件安全
第五天	CISP0207	安全漏洞及恶意代码	恶意代码基本概念及原理、防御技术
			信息安全漏洞/安全攻防基础
	CISP0208	安全攻防实践	目标信息收集/密码破解原理与实践
			缓存溢出原理与实践
			电子欺骗攻击原理与实例
			拒绝服务攻击原理与实例
			网页脚本漏洞原理与实例
第六天	CISP0301	信息安全管理体系	信息安全管理基本概念
			信息安全管理体系建设
	CISP0302	信息安全风险管理	风险管理工作内容
			信息安全风险评估实践
第七天	CISP0303	信息安全管理措施	安全基本管理措施
	CISP0304	重要安全管理过程	重要安全管理过程
第八天	CISP0501	信息安全标准与法规概况	信息安全法规与政策概况
			重点信息安全法规和政策文件解读
			信息安全道德规范
			安全标准化概述
			信息安全管理标准ISMS/
			信息安全评估标准CC
	CISP0209	软件安全开发	等级保护标准
			软件安全开发概况
			软件安全开发的先锋阶段

传统体系化的培训课程设计



培训服务课程体系

教学思路

SQL注入的教学怎么教？

传统教学顺序

第一步：ASP/PHP/JAVA语言
第二步：SQL语法及数据库
第三步：　SQL注入的原理
第四步：　SQL注入实验

问题来了

为什么很多安全大牛的学历并不高？

为什么很多高中或职学生反而学的快？

为什么大学教育的学生毕业无法满足企业要求？

传统教学顺序

信息安全较难

课程压力已经磨灭了兴趣

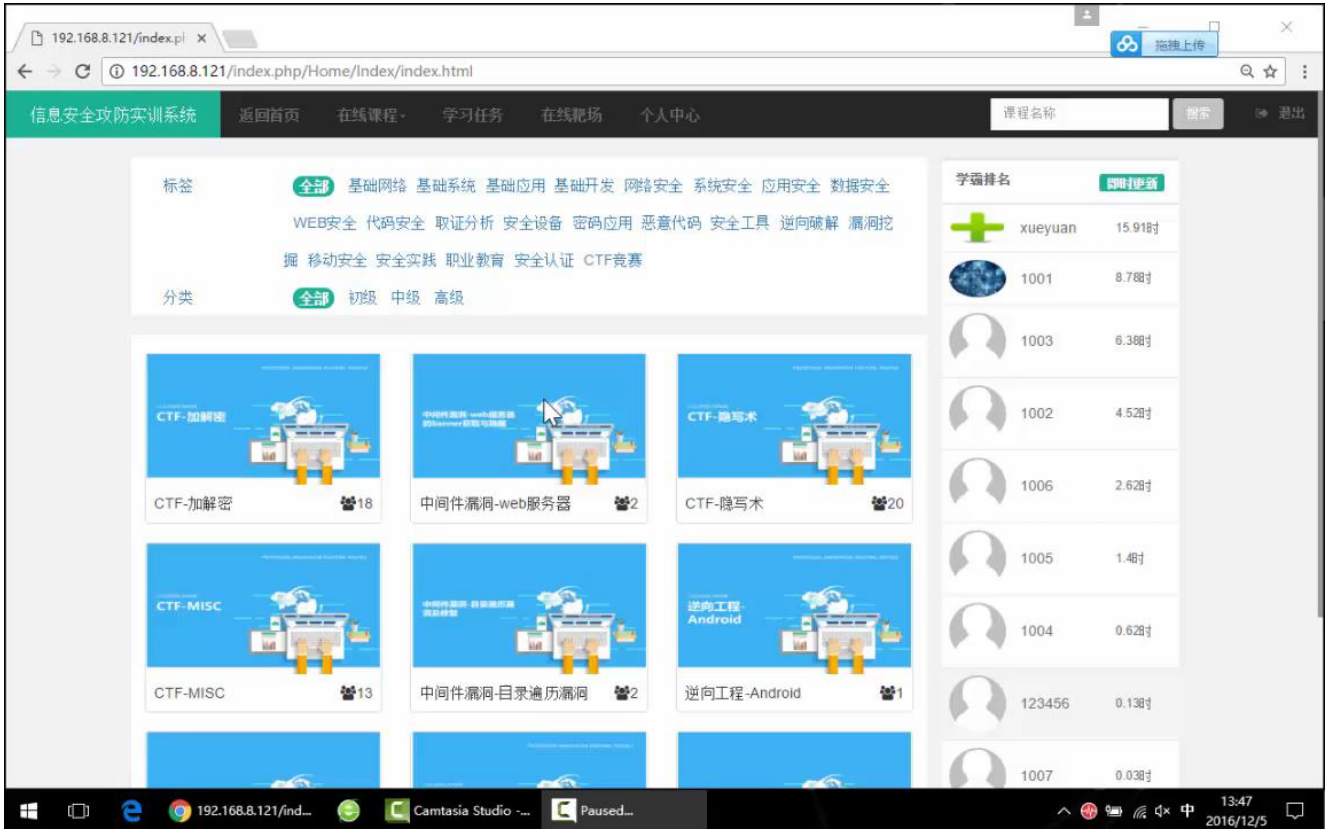
教师压力大

更新快

问题

考驾照怎么考的？
第一天做什么？

如果先操作再学习？



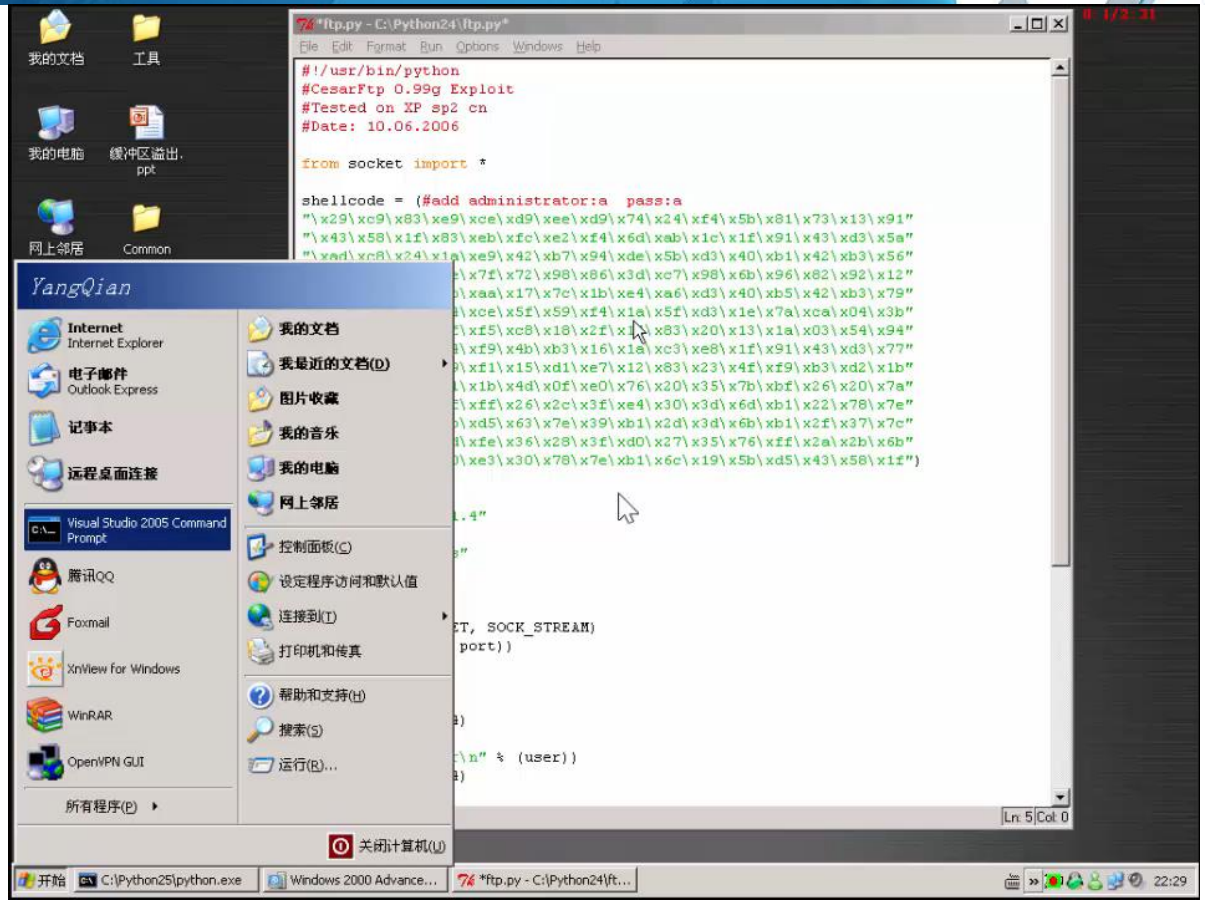
教学思路

缓冲区溢出的教学怎么教？

传统教学顺序

第一步：C或C++语言
第二步：计算机系统结构
第三步：汇编语言
第四步：堆溢出与栈溢出
第五步：FUZZ技术
第六步：溢出实验

先做溢出实验如何？



教学思路

浏览器溢出的教学怎么教？

传统教学顺序

第一步：C或C++语言
第二步：计算机系统结构
第三步：汇编语言
第三步：HTML、CSS、Javascript
第四步：堆溢出与栈溢出
第五步：FUZZ技术
第六步：浏览器保护bypass技术
第七步：溢出实验

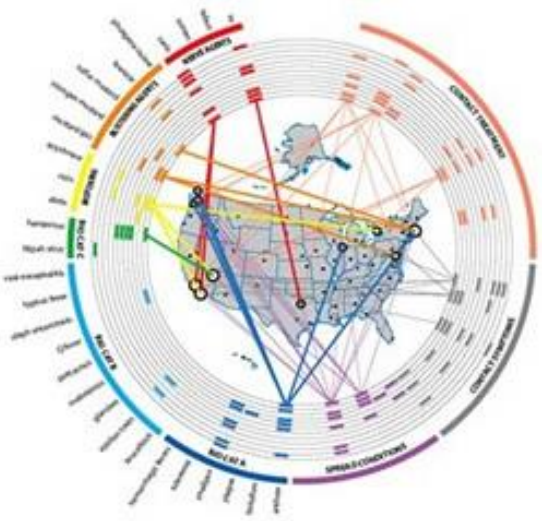
先知道结果更重要

LAB

信息安全实验室建设

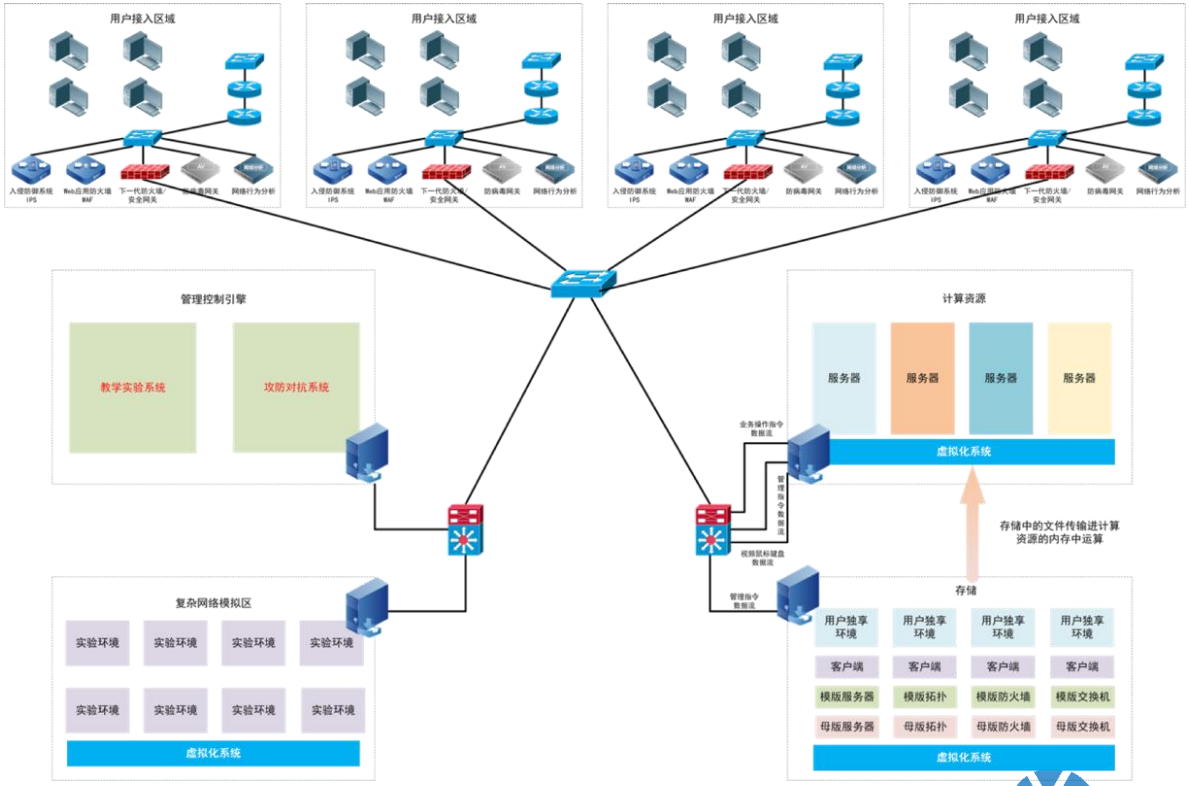
攻防仿真

信息安全的核心内容在于信息攻防，通过对实验环境组合，能构建300~500余个实验，涉及各类安全工具使用教学、网络攻防、Web攻防、漏洞发掘和防护等各项内容。

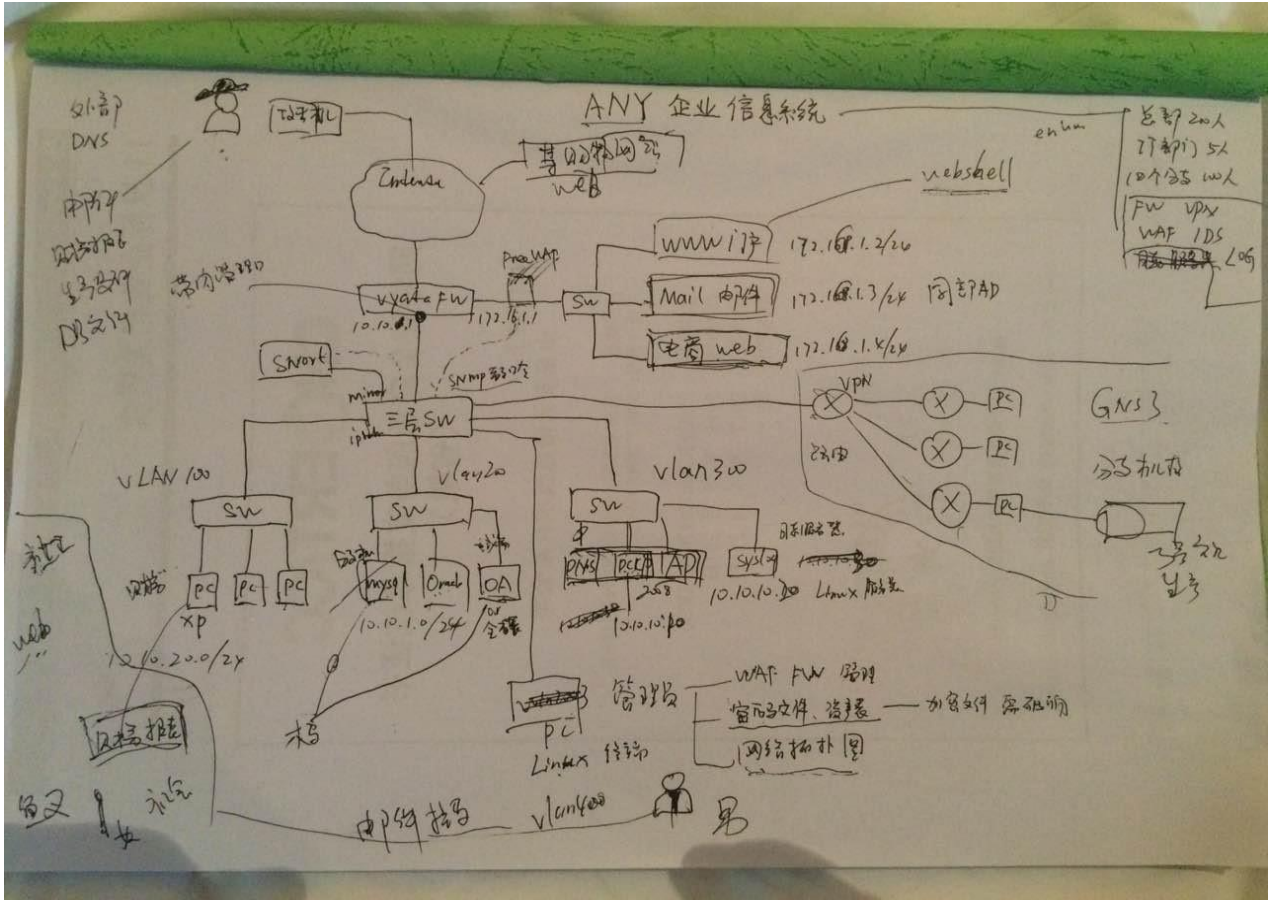


技术架构

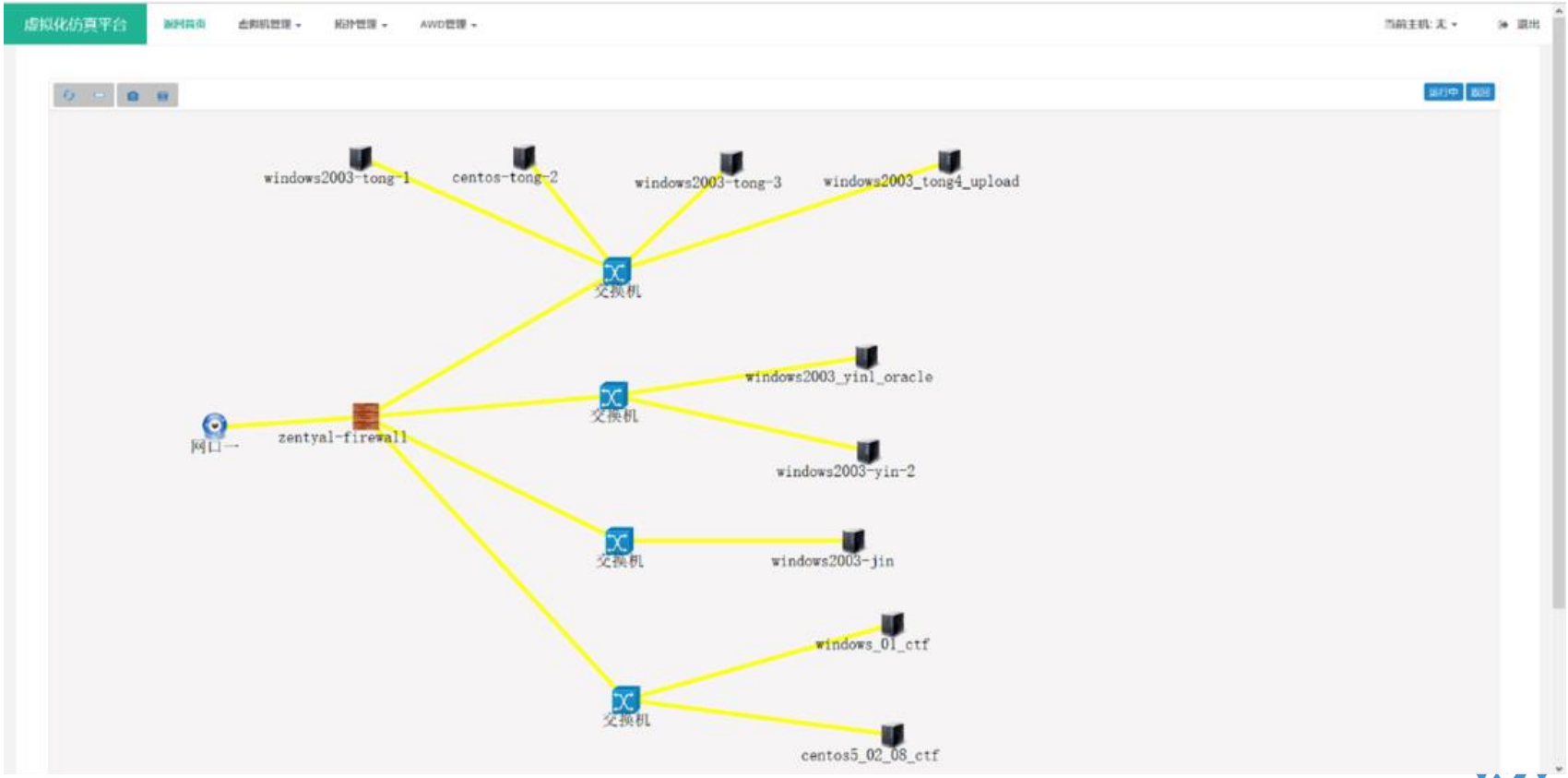
- 实验室由控制引擎、计算资源、存储资源和基础网络设备、实验安全设备组成
- 采用虚拟化和软件定义网络技术
- 软件仿真各类实验环境
- 丰富系统的安全课程和实验并保持更新



攻防仿真



攻防仿真



实训课程

信息安全攻防实训系统 | 返回首页 | 在线课程 | 学习任务 | 在线靶场 | 个人中心 | 退出

全部课程 / 逆向工程-客户端 初级课程

逆向工程(又称逆向技术)，是一种产品设计技术再现过程，即对一项目标产品进行逆向分析及研究，从而演绎并得出该产品的处理流程、组织结构、功能特性及技术规格等设计要素，以制作出功能相近，但又不完全一样的产品。逆向工程源于商业及军事领域中的硬件分析。其主要目的是在不能轻易获得必要的生产信息的情况下，直接从成品分析，推导出产品的设计原理。 逆向工程可能会被误认为是对知识产权的严重侵害，但是在实际应用上，反而可能会保护知识产权所有者。例如在集成电路领域，如果怀疑某公司侵犯知识产权，可以用逆向工程技术来寻找证据。

学习进度 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

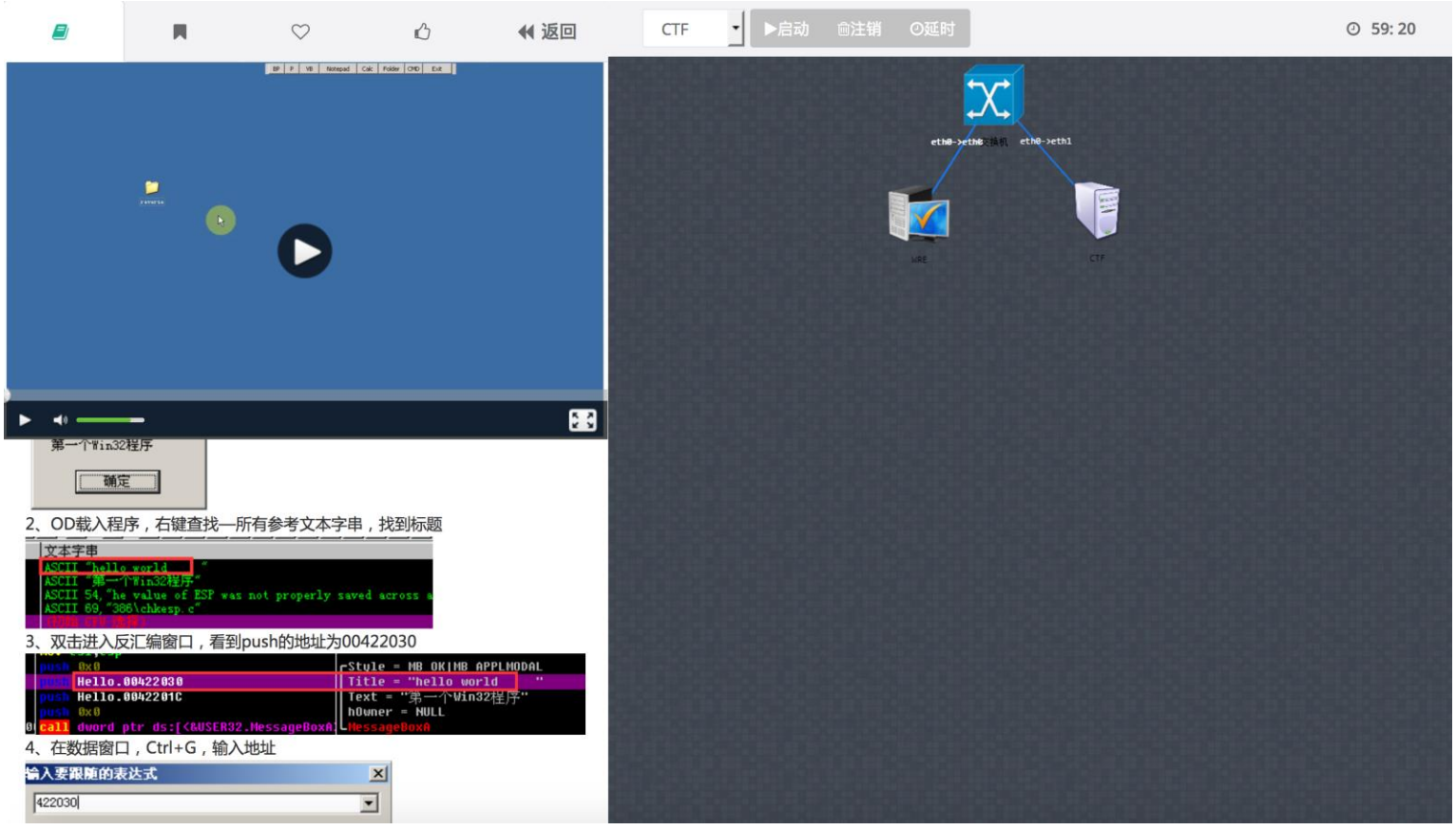
课时列表

OllyDbg:1修改程序标题
0.07学时

OllyDbg:2TraceMe程序爆破
0.04学时

OllyDbg:3ReverseMe程序爆破
0学时

实训课程



COMPETITION

信息安全学科竞赛

竞赛模式

闯关答题模式：设置多个难度不同的题目，比赛者将答案填写正确即可得分，最后统计分数排行。

答题闯关模式

CTF(Capture The Flag)：中文一般译作夺旗赛,在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。

THE END

http://www.yxlink.com
南京铱迅信息技术股份有限公司

Security Powers The Internet