广西科技大学启迪学院

《信息安全第二阶段实施方案》

项目知识概要

1. 网络安全攻防技术
2. Web渗透测试
3. 主机渗透测试
4. 无线安全
5. 安全防护
6. 靶场训练

项目

1、Web渗透测试靶场实战
2、安全攻防夺旗实战

目　录

第一章 信息安全专业学习背景 3
1.1 中国信息安全产业空间高速增长 3
1.2 信息安全专业人才急缺 4
1.3 人才就业方向 4
1.4 产业大发展，待遇水涨船高 5
第二章 信息安全专业培养对象及目标 6
2.1. 培养对象 6
2.2. 培养目标 6
第三章 信息安全专业第一阶段培养技术内容 7
3.1. 培养技术内容简介 7
3.2. 渗透测试实战靶场预览 8
3.2.1.Web渗透测试靶场 8
3.2.2.CTF模拟练习靶场 8
3.3. 项目部分内容描述 9
3.3.1.Web渗透测试靶场基本介绍.....9
3.3.2.CTF练习靶场 9
第四章 信息安全培养第二阶段时间安排 9
第五章 关于我们 11
5.1. 公司简介 11
附注 11

第一章 信息安全专业学习背景

1.1 网络信息安全行业发展形势分析

（一）国家层面对网络信息安全高度重视，行业发展迎来新高度

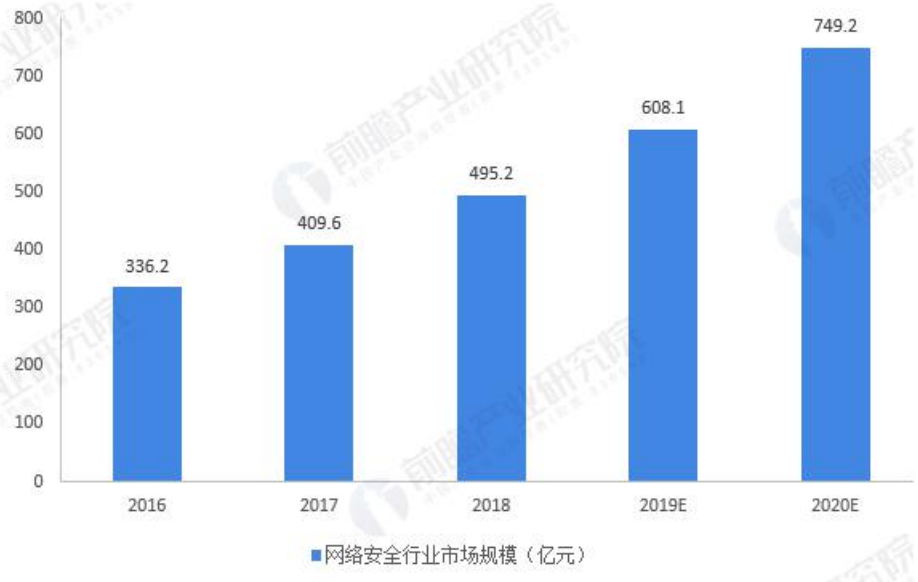
2014年2月27日，中央网络安全和信息化领导小组成立。习近平指出，“没有网络安全就没有国家安全，没有信息化就没有现代化。”国家互联网信息办公室于2016年底发布了《国家网络空间安全战略》，这是我国首次发布关于网络空间安全的战略。2019年上半年，发生在我国网络安全事件和威胁情况进一步加剧，各类网络安全事件数量占比仍然较高。2019年我国比较典型的网络安全事件包括：2019年3月，境外黑客利用勒索病毒攻击部分政府和医院机构;华为起诉美国政府，称其涉嫌入侵华为服务器; 2019 年1月，超2亿的中国求职者简历泄露，不受保护状态持续一周等。

在国家层面上，2019年两会期间，政府工作报告也多次提及信息安全。高层高度关注网络安全，从立法到全网络安全检查以及网络安全国际合作，利好集中释放，有利于推动行业高速成长。

（二）网络安全威胁推动行业发展，网络安全行业规模有望超700亿

随着信息化的快速发展，信息安全产业市场空间不断扩大，政府和企业均越来越重视信息安全，用户法规遵从要求越来越高，企业投入逐步增加，安全产品更具自主创新性并且更加多元化。强劲的市场需求推动信息安全产业规模快速增长，2019年产业规模超过600亿元，年增长率超过20%，明显高于国际8%的平均增数，保持健康的发展态势。随着对网络安全的愈加重视及布局，市场规模将持续扩大，到2021 年中国网络安全市场规模将达千亿元。

图表3：2016-2020年中国网络安全行业市场规模(单位：亿元)



资料来源： 中国信通院 前瞻产业研究院整理

信息安全企业的数量和规模也有了较大提高，截至2019年底，国内信息安全相关企业已超过千家，另一方面，信息安全产品种类不断丰富，安全操作系统、安全芯片、安全数据库、密码产品等基础技术产品逐步成熟，防火墙、病毒防护、入侵检测、终端接入控制、网络隔离、安全审计、安全管理、备份恢复等网络安全产品服务取得明显进展，产品功能逐步向集成化、系统化方向发展。

网络安全行业的发展短期内是通过频繁出现的安全事件驱动，短中期离不开国家政策合规，中长期则是通过信息化、云计算、万物互联等基础架构发展驱动。2020年网络安全领域进一步迎来网络安全合规政策及安全事件催化，例如自2020年1月1日起施行《中华人民共和国密码法》，2020年3月1日起施行《网络信息内容生态治理规定》等。2021年作为“十三五”收官之年，将陆续开始编制网络安全十四五规划。在各种因素的驱动下，我国网络安全行业将得到进一步发展。

1.2 信息安全人才现状：面临全球性“人才荒”

从总体上看，我国网络安全人才还存在数量缺口较大、能力素质不高、结构不尽合理等问题，与维护国家网络安全、建设网络强国的要求不相适应”。即将实施的《网络安全法》第二十条也明确表示：“国家支持企业和高等院校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流”。

麦可思研究院发布《2020年中国大学生就业报告》，对2016-2020届毕业生就业量前120位的专业就业满意度较高的前十位本科和高职高专专业进行了研究分析，报告显示，在本科专业，“信息安全”专业本科毕业生就业满意度连续两年排名居首。

安全领域火爆的原因是安全人才的抢手，薪酬水平也直线上升。毫不夸张的说，网络安全是一份很有“钱”途的职业。网络安全专业凭借其高薪资、广阔的行业前景、极高的就业率俨然已经成为毕业生们优先选择的“香饽饽”。WEB开发工程师平均年薪最高，为48.60万元。

1.3 人才就业方向

网络信息安全专业学生毕业后可在政府机关、国家安全部门、银行、金融、证券、通信领域从事各

类信息安全系统、计算机安全系统的研究、设计、开发和管理工作，也可在IT领域从事计算机应用工作，由于国内信息安全专业人才的紧俏，这一行业的起薪相对较高。相关职业岗位及典型工作任务如下表。

序号	工作岗位	岗位工作内容描述	职业素质与能力要求
1	信息安全/安全运维工程师	1.熟悉渗透测试的各类技术及方法，熟练掌握各种渗透测试工具；熟练操作各类操作系统、应用平台； 2.熟悉网络技术TCP/IP协议、HTTP协议，广泛理解各类网络、主机、数据库、Web安全知识技术技能和攻防手段； 3.掌握各类开源的安全漏洞检测扫描、安全防范、安全渗透测试、安全审计及信息管理工具； 4.熟悉防火墙、IDS/IPS、WAF、SIEM等主流安全产品及解决方案 5.熟悉主流Web安全技术，熟悉常见攻击和防御办法，自行进行web渗透测试，恶意代码监测和分析； 6.具有团结协作精神,以及良好的沟通和口头(文字)表达能力，学习能力强，能承受较强工作压力。	1.职业素质：信息安全建设、管理，网络安全评估及检查 2.能力要求： ●网络的安全设备安装和调试能力 ●服务器及网站日志审查能力 ●安全漏洞的跟踪、安全审核能力 ●安全风险评估与分析及加固能力 ●安全文档的书写能力 ●响应安全事件能力
2	渗透测试工程师	1.熟悉渗透测试步骤、方法、流程，熟练使用一定量的渗透测试工具； 2.熟悉攻击的各类技术及方法，对各类操作系统、应用平台的弱点有较深入的理解； 3.熟悉常见脚本语言，能够进行WEB渗透测试，恶意代码检测和分析； 4.有一定代码编写能力 5.主动性强，具有良好的沟通、	1.职业素质：承接的渗透测试项目，跟踪安全动态，信息安全风险应急响应工作。 2.能力要求： ●跟踪国际/国内安全社区的安全动态，进行安全漏洞分析、研究与挖掘，并进行预警能力； ●协助做好信息安全风险应急响应工作； ●编写渗透测试报告和对客户进行信息安全培训； ●完成安全评估任务和评估报告的编写工作。

		协调和组织能力和文档编写能力，逻辑性强。	
3	等级保护测评工程师	1.有较好的安全理论基础，掌握主流安全产品的原理和应用； 2.掌握信息安全等级保护和风险评估技能 3.掌握安全应急响应知识； 4.熟悉主流信息安全规范，如ISO27000； 5.具备良好的文档编写能力； 6.具有团结协作精神,以及良好的沟通和口头(文字)表达能力和服务意识	1.职业素质：信息安全等级保护，信息安全审计，信息安全认证 2.能力要求： ●信息安全等级保护的评估与咨询能力； ●信息安全风险评估的咨询与服务能力； ●信息安全应急响应的咨询与服务能力； ●ISO27001认证咨询与服务能力。
4	安全服务工程师	1.掌握防火墙、VPN等安全产品的原理和应用维护知识和技能； 2.掌握入侵检测系统的原理和应用维护知识和技能； 3.具备一定的网络隔离技术； 4.有较好的安全理论基础，熟悉PKI、SSL等安全技术 5.具备一定的程序开发的能力。	1.职业素质：安全产品系统测试，安全产品的需求分析、功能定义 2.能力要求： ●安全产品系统测试方案设计和实施能力； ●安全产品的需求分析和功能定义能力； ●跟踪记录及推动问题的及时解决能力； ●编写、整理文档能力。
5	售前工程师	1.熟悉网络安全产品的相关知识； 2.具有良好的语言表达能力和快速应变能力； 3.具有资料收集与整理的能力、文字处理能力、数据分析能力； 4.具有团结协作精神,以及良好的沟通和口头(文字)表达能力和服务意识	1.职业素质：销售、售后服务与技术支持 2.能力要求： ●市场考察，发掘及选择顾客能力； ●演示产品，制订报价单能力； ●编写技术方案、合同草案文本能力； ●协助处理与客户方的联络及关系协调能力； ●管理及统计客户信息资料能力； ●接受用户上报系统问题，分析记录、解答、上报问题，满意度回访能力。
6	系统工程师/实施工程师/技术	1.熟悉当前流行操作系统(如windows、Linux等系统)的应用及安全机制和相关配	1.职业素质：信息安全管理方案的设计和实施，安全咨询和服务，电子商务网站的安全管理

	支持工程师	置 2.有扎实的网络基础专业知识和网络互联设备及网络安全设备的应用维护能力； 3.具备一定的风险分析、防病毒和安全策略制定的能力； 4.具备较强的信息安全意识和安全管理能力。 5.编写、整理技术文档	2.能力要求： ●方案概要设计能力； ●模块级详细设计能力； ●简单的排错及编写能力； ●编写、整理技术文档能力。

第二章 信息安全技术培养对象及目标

2.1.培养对象

- ✓ 信息安全技术热爱者，高校相关计算机专业方向
- ✓ 追求稳定高薪且意愿进军 信息安全“顶端食物链”
- ✓ 对代码”过敏”，没有良好代码的设计能力的伪开发者
- ✓ 意愿将 信息安全 技能工作作为终极职业生涯发展者

2.2.培养目标

为满足社会经济各领域对信息安全人才的需求，需要在信息安全基础建设、管理、应用技术开发等多个层次进行人才的培养。培养具有系统安全管理与应用分析能力、掌握信息安全应用趋势的高端技能型专门人才。学生通过学习掌握操作系统安全知识，具备操作系统安全管理与维护能力，学习掌握安全设备部署及应用知识，具备网络安全管理、应用、维护能力，学习掌握Web安全技术知识、主机渗透测试技术知识、内网渗透测试技术知识，具备渗透测试攻击及防护能力，学习掌握python安全开发技术知识，具备安全应用设计与开发能力，学习掌握CTF攻防夺旗知识，具备高级信息安全应用、管理能力。

毕业生目标工作岗位是系统安全工程师、网络安全工程师、渗透测试工程师、安全运维工程师，主要从事系统安全运维、Web渗透测试、代码安全分析、系统安全审计等岗位，需要具备的知识是操作系统安全知识、网络安全知识、渗透测试知识、安全编程知识，能够完成安全设备部署及应用，安全工具设计与开发实现，网站渗透测试，内网渗透测试，应急响应。

第三章 信息安全技术第一阶段培养技术内容

3.1.培养技术内容简介

1、基础：安全攻防基础概念、网络信息收集、发现并探测主机信息

2、基础：Web服务器搭建、OWASP TOP 10详解、SQL注入

3、基础：BurpSuite实战、文件上传漏洞、网站木马、代码分析及防护

4、基础：解析漏洞、编辑器漏洞利用、Cookie欺骗

5、基础：XSS攻击实战、CSRF攻击实战、项目实战演练（XSS+CSRF组合攻击）

6、进阶：SQL盲注、SQL时间延迟注入、SQL注入项目实战

7、进阶：命令执行、Cookie注入、文件包含漏洞

8、进阶：SQL注入进阶、XSS进阶

9、进阶：Web密码破解、主机协议密码破解、无线密码破解、其他密码破解、字典生成工具

10、进阶：Windows主机安全、 Linux主机安全、数据库安全配置

11、进阶：拒绝服务攻击、协议欺骗攻击

12、进阶：社会工程学、钓鱼攻击

13、高级：木马病毒分析以及手动查杀

14、高级：主机漏洞利用、后渗透攻击

15、高级：漏洞利用工具进阶使用、“心脏滴血”漏洞利用

16、高级：远程执行漏洞复现、主机漏洞加固

17、高级：CTF介绍、CTF专项讲解

18、高级：CTF题目专项练习、专项练习讲解（一）

19、高级：CTF题目专项练习、专项练习讲解（二）

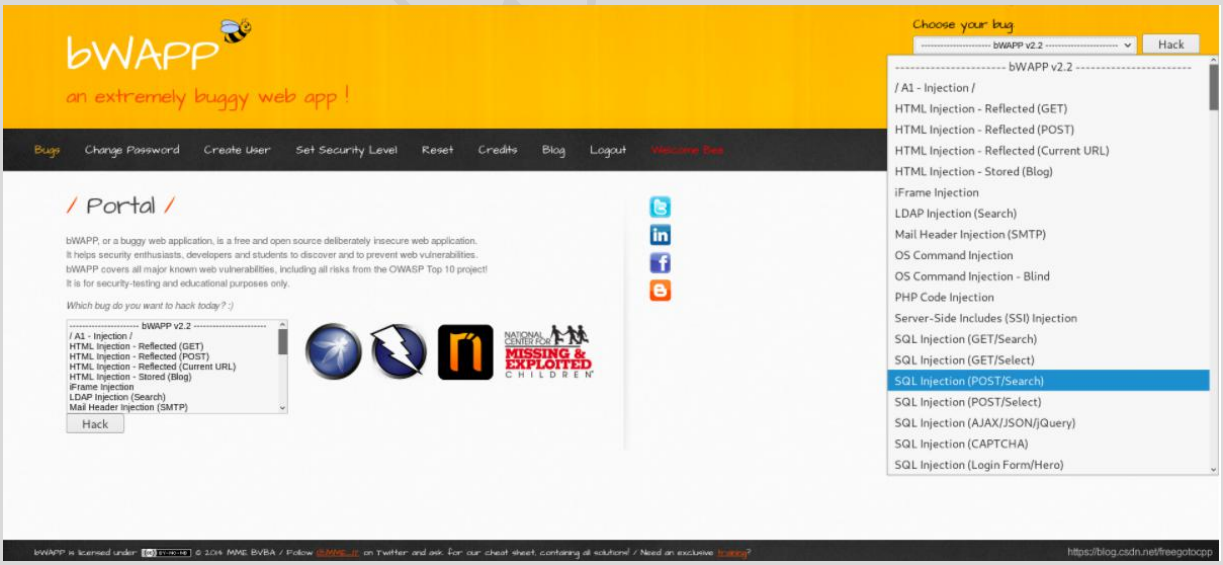
20、课程总结、项目考核

3.2.渗透测试实战靶场预览

3.2.1.Web渗透测试靶场

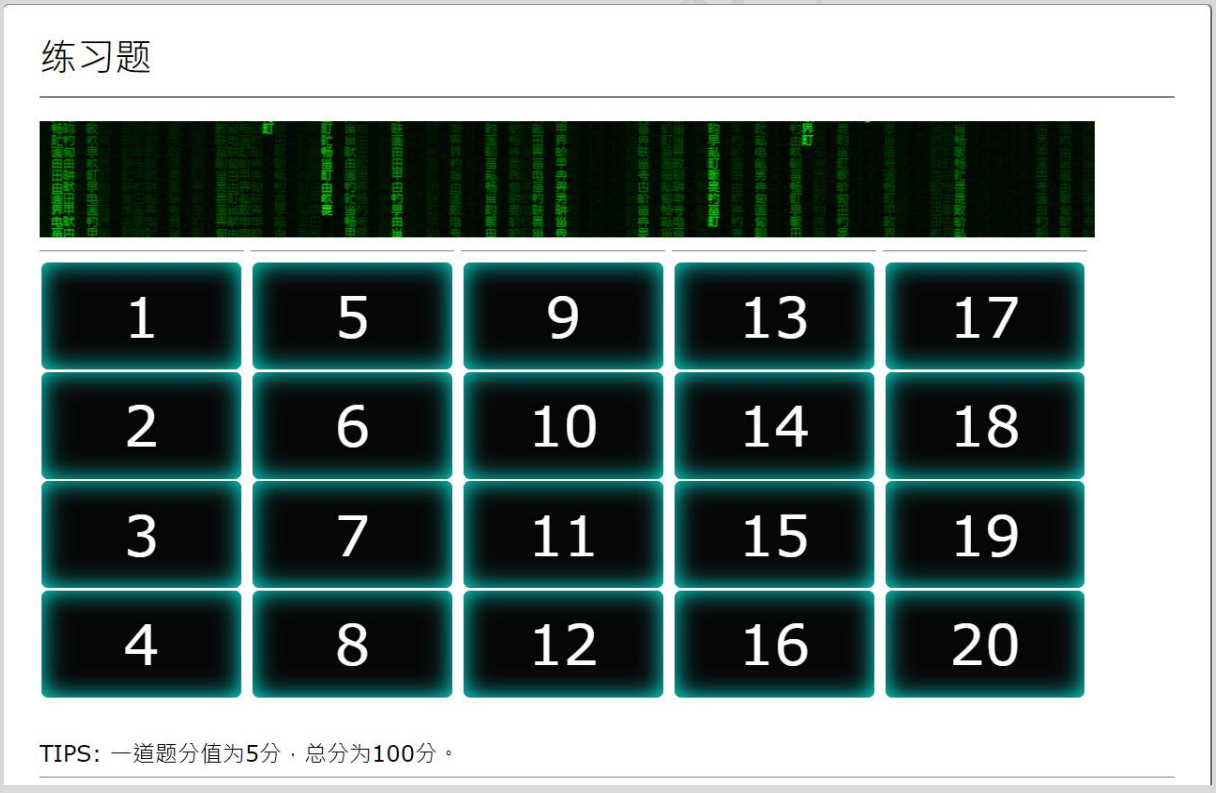
①部署安装bWAPP靶场

②选择指定靶场进行练习



③对漏洞进行攻击

3.2.2.CTF模拟练习靶场



3.3.项目部分内容描述

3.3.1. Web渗透测试靶场基本介绍

bWAPP（buggy web Application） 是一个集成了各种常见漏洞和最新漏洞的开源Web应用程序，目的是帮助网络安全爱好者、开发人员和学生发现并防止网络漏洞。包含了超过100种漏洞，涵盖了所有主要的已知Web漏洞，包括OWASP Top10安全风险，最重要的是已经包含了OpenSSL和ShellShock漏洞。

3.3.2.CTF练习靶场

CTF靶场是一个综合了多个信息安全领域的训练题目，本套练习题为入门级CTF比赛题型，内置20道题目，其中包含：信息泄露、文件上传、XSS、SQL注入、图片隐写、音频隐写、越权漏洞、弱口令、日志分析、安全杂项等题目类型。适合于CTF初学者、学生进行训练。从而提升相应领域的操作技能。

第四章 信息安全培养第二阶段时间安排

时间	内容
Day1	常见黑客攻击手段、渗透测试流程、渗透测试平台；常见信息收集技巧、高级搜索Google Hacking、Web扫描、主机漏洞扫描。
Day2	动态网站部署(phpstudy、xampp)、DVWA、bWAPP靶场。SQL手工注入、SQL工具注入。
Day3	常见Burpsuite模块的使用、 黑名单校验、白名单校验、MIME、文件头校验、网站木马、代码分析及防护
Day4	IIS解析漏洞、Apache解析漏洞、Nginx解析漏洞、解析漏洞防护、编辑器漏洞利用、漏洞修复、利用Cookie欺骗获取用户信息
Day5	利用XSS漏洞获取用户cookie、CSRF攻击实战、项目实战演练（XSS+CSRF组合攻击）

Day6	SQL盲注、SQL时间延迟注入、SQL注入项目实战
Day7	命令执行、Cookie注入、文件包含漏洞
Day8	SQL注入进阶：二阶注入、宽字节注入、特殊注入方法、SQL-Lab闯关练习；XSS进阶：XSS绕过方法、特殊XSS语句、XSS-Lab闯关练习。
Day9	Web密码破解、主机协议密码破解、无线加密原理、无线破解工具Aircrack-ng、Fern wifi cracker、Wifite、Office文件破解、RAR压缩文件破解、木头字典生成器、Crunch、Rtgen。
Day10	Windows常用安全配置、Linux安全概述、Linux主机加固（账号安全配置、权限安全配置）、数据库安全配置
Day11	拒绝服务攻击、 Dos攻击、CC攻击、通过python脚本实现DDoS攻击。
Day12	社会工程学理论、SET社会工程学工具包、社工库；WIFI钓鱼攻击、邮件钓鱼攻击、文件钓鱼攻击。
Day13	木马病毒分析以及手动查杀、 木马远程监控、木马病毒文件分析、木马病毒的隐藏位置以及如何查杀
Day14	Metasplit Framework详解、Mepterprepter介绍、MS08-067、MS12-020、MS16-016漏洞利用、权限提升、木马监控、植入后门、清除痕迹
Day15	漏洞利用工具进阶使用、MSF攻击数据库服务、MSF攻击PDF文件、利用borwser_autopwn渗透模块攻击浏览器、免杀Payload生成工具Veil。“心脏滴血”漏洞讲解、Linux下“心脏滴血”漏洞检测、“心脏滴血”漏洞加固。
Day16	CVE-2019-0708漏洞复现、其他各种远程命令执行漏洞复现、勒索攻击复现、主机漏洞加固、防火墙加固、漏洞修复加固
Day17	CTF介绍、CTF题目类型、CTF解题思路、CTF解题工具、Crypto（密码学基础、常见编码类型、文本加密、换位加密、替换加密、代码混淆加密）、Misc（取证技术、隐写术、脑洞类型）。
Day18	CTF题目专项练习、专项练习讲解。
Day19	CTF题目专项练习、专项练习讲解。
Day20	课程总结、项目考核。

第五章 关于我们

5.1. 公司简介

➢ 尚观科技有限公司：

- 尚观科技，成立于 2005 年，由一批“IT 愤青”创建，在高端技术教育领域深耕 至今 15 年。
- 技术为王，是尚观体内始终流淌的血液，课程每 6 个月更新一次，坚持以一线最新技术为指引。
- 在尚观人共同努力下，如今在北京、上海、深圳、沈阳、大连、成都、广州、西安、武汉等地均设有近千平米教室的高端 IT 培训公司。
- 多年获得 RedHat 及 Oracle 在中国最大最佳授权合作伙伴殊荣
- 成为国内数百所高校校企合作的优秀典范
- 国内外数百家大型 IT 互联网企业深度合作单位

附注：

近年来，网络安全已成为事关经济社会发展、国家长治久安和人民群众福祉的重大战略问题，建立一支有规模、结构优化、素质优良的网络安全人才队伍已成为维护国家网络安全和建设网络强国的核心需求。我们也坚信在生活中未来的网络信息安全会越来越重要。

考虑到广西科技大学启迪学院实训为持续的阶段性，且每阶段的课时相对比较充分，因此，实训二的课程设计旨在将参加实训的同学打造为信息安全初级工程师水平，为打造第三阶段中高级信息安全工程师奠定扎实的基础。这样下来确保连续参加信息安全实训的同学可以轻松的跨入新一代的信息安全工程师的队伍。