**信息安全拔尖班选拔办法**

为深化产教融合，拓展多元化办学体制，全面推行校企协同育人，实现教育改革和产业发展统筹融合，四川轻化工大学与深信服科技有限公司在网络与信息安全专业方面开展深层次校企合作，致力建成四川省一流网络安全人才培养品牌，成为深信服科技有限公司网络安全人才战略中应用型人才的重要标杆。

同时，本办法还为进一步加强信息安全拔尖班管理，遴选有一定信息安全的理论水平、实践能力和较强的综合素养的网络与信息安全优秀学生，以进一步把学生培养成一批社会需要的，具有扎实的理论基础、突出的工程实践能力、较高的综合素质的拔尖创新工程应用型人才；结合我院的实际情况，特制定本办法作为信息安全拔尖班招新总成绩评定依据。

一、热爱祖国，拥护中国共产党领导，立志成为又红又专的网络空间安全人才。

二、信息安全拔尖班每年计划在大学本科二年级学生中录取20-30名的学生，招录学生按总成绩由高到低排名确定。

三、总成绩由平均学分绩点、综合素质加分、初试考核成绩、面试成绩四项成绩确定。

四、总成绩得分计算办法：总成绩=平均学分绩点标准化\*20%+综合素质分标准化\*10%+初试考核成绩标准化\*40%+面试成绩标准化\*30%。

附：每项成绩的标准化公式为：。

五、综合素质分评定办法，见附件1。

六、初试主要考核学生的信息安全理论水平。根据情况选择以下之一考核方式。

考试方式（一）：初试考核的标准依据深信服1+X认证“网络安全运营平台管理”初级认证级别，学生在完成相应的课程学习之后，参加由深信服统一命题和组织的初级认证考核。考核的题型包括但不限于：选择题、判断题、实操题等，初试考核课程模块及大纲见《附件2.1 信息安全拔尖班初试选拔课程模块及大纲》。

考试方式（二）：初试考核的标准依据国家信息安全水平考试（NISP）一级认证级别，学生参与相应的课程学习及习题练习后，参加由信息安全拔尖班统一组织和命题的认证考核。考核的题型包括但不限于：选择题、填空题、判断题、简答题等，初试考核大纲见《附件2.2 NISP（一级）考核内容及要求》。

考试方式（三）：初试考核的标准依据长城网络靶场竞技系统，学生参与相应的课程学习及习题练习后，参加由信息安全拔尖班统一组织的考核。考核的题型包括但不限于：基础理论考核题、夺旗闯关考核题、主机渗透题等，初试考核大纲见《附件2.3 长城网络靶场竞技系统考核大纲》。

七、面试主要根据学生的成绩表、申请表、奖证材料、初试考核情况、信息安全理论水平、信息安全动手实践能力、个人综合素质等方面综合考察，择优录取。面试考核问答参考题见附件3。

八、拔尖班招新选拔流程为：

1、填写报名申请表、教务系统下载的电子版成绩单、相应辅助证明材料的电子扫描件（如相关证书、奖状、专利论文等），打包发送至招生负责人的邮箱。（负责人：李同，E-mail：litong@suse.edu.cn）

2、选拔QQ群公布参与信息安全初试考核考核安排。

3、组织信息安全初试考核。

4、公布面试名单和面试选拔考核安排。

5、组织面试考核。（面试评委：由拔尖班培养团队成员和相关专家组成面试团队完成选拔考核工作。）。

6、公示录取名单。

7、建立拔尖班学生学籍档案。

**附件1 综合素质分加分指标体系**

一、学生干部加分（多重身份者，取最高分，其他多一项职务多加0.01分）

（一）担任各班团支书、班长加0.10分，副班长、学习委员、心理委员加0.08分，其他班委加0.05分；

（二）担任校院级团总支副书记、学生会主席加0.20、副主席加0.18分，部长加0.15分、副部长加0.12分,干事加0.08分；

（三）院级以上学生团队（例如：蒲公英志愿者服务队、艺术分团等），总负责人加0.18分、副职总负责人加0.15分，下设部（队）长加0.12分，下设副部（队）长加0.10分，下设干事加0.08分；

（四）学生党支部副书记加0.15分、支委成员或支部书记助理加0.08分；

（五）校院级社团或协会，总负责人加0.15分、副职总负责人加0.12分，下设部长加0.10分，下设副部长加0.08分，下设干事加0.05分.

二、学生参加活动情况加分

（一）相关科技活动

1、在一般期刊上发表学术论文者加0.20分，在核心期刊上发表论文者加0.50分；

2、成功申报科研项目，项目负责人校级加0.15分、省级以上加0.30分，项目组成员加0.05分；

3、获三等奖以上的奖励，校院级加0.20分，省级加0.40分，国家级加0.6，获省级以上优秀或优胜奖加0.20分（省级以上含名企举办的科技竞赛），获校院级优秀奖加0.10分。

4、参加科技竞赛（网页设计竞赛、挑战杯竞赛、CTF等）成功提交作品未获奖者加0.05分。

5、鼓励学生参加教师科研项目研究，项目成员加0.10分。

6、参与各类学术讲座，院系级加0.03分，校级加0.05分，省部级0.08分。

7、科研项目结题，项目负责人校级加0.15分、省级以上加0.30分，项目组成员加0.05分；

8、获国家专利局授权的创造发明证书者加0.80分；获实用新型、软件著作权、外观设计等证书者加0.30分；

三、学生参加技能测试情况加分

（一）全国大学生英语四、六级考试成绩425分以上,四级加0.10分、六级加0.15分；

（二）通过全国计算机三级考试加0.05分、四级考试加0.15分；

（三）获计算机技术与软件专业技术资格（水平）考试资格证书，初级加0.05分、中级加0.15分、高级加0.30分；

（四）获其它专业资格证书，初级加0.05分、中级加0.15分、高级加0.30分。（nisp一级按初级证书加分0.15，二级按中级证书加分0.30）。

（五）参与技能培训，1-3天加0.03分；4-10天加0.05分，10天及以上加0.08分。

四、学生受表彰情况加分

（一）院系级表彰，加0.1分，校级表彰加0.2分，省部级表彰加0.4分。（如，三好学生，优秀团员，奖学金等）。

五、其他需要加分的情况，学生本人提交申请，拔尖班负责人审批认定。

**附件2.1** **信息安全拔尖班初试选拔课程模块及大纲**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **网络安全运营平台管理 课程大纲** | | | | |
| **序号** | **认证**  **级别** | **课程模块** | **知识点/大纲** | **课时（天）** |
| 1 | 初级 | 1+X-网络安全法律法规 | 网络安全法背景概述 网络安全法解读 相关案例分析及法律责任 | 0.5 |
| 2 | 1+X-网络协议基础 | 数据包分析战-Wireshark基础 数据包分析战-过滤器 数据包分析战-数据统计 网络协议攻击与防御-应用层协议攻击与防御 | 0.5 |
| 3 | 1+X-操作系统基础 | Windows操作系统基础-基础介绍与安装 Windows操作系统基础-DNS服务介绍 Windows操作系统基础-DNS服务器搭建与配置 Linux操作系统基础-命令行基础 Linux操作系统基础-文件系统和目录 Linux操作系统基础-文件权限管理 Linux操作系统基础-VIM文件编辑器 | 0.5 |
| 4 | 1+X-HTTP协议 | HTTP协议-基础 HTTP协议-特点 HTTP协议-请求方式 HTTP协议-请求响应过程 HTTP协议-HTTPS扩展 | 0.5 |
| 5 | 1+X-渗透测试工具使用 | 渗透测试工具使用-Nmap 渗透测试工具使用-BurpSuite 渗透测试工具使用-Metasploit | 1 |

**附件2.2 NISP（一级）考核内容及要求**

|  |  |  |  |
| --- | --- | --- | --- |
| 知识体 | 组成部分 | 考核标准 | |
| 要求 | 内容 |
| 信息安全基础 | 第一部分： 信息安全概述 | 识记 | 信息和信息技术的概念；信息技术的发展阶段及各阶段的主要特点；信息安全基本属性及含义；信息安全的特征；信息安全保障的概念和作用；信息系统、风险和使命的关系；信息系统安全保障概念和关系；信息安全保障模型 |
| 领会 | 信息安全问题产生的根源；信息系统安全保障模型中保障要素、生命周期和安全特征的内容和含义 |
| 第二部分： 信息安全法律法规 | 识记 | 国家秘密的概念和分级；危害国家秘密的犯罪行为；商业秘密和个人信息的概念；《网络安全法》、《数据安全法》、《个人信息保护法》、《密码法》中关于网络与信息安全的主要条款；网络违法犯罪的概念；《关于维护互联网安全的决定》、《中华人民共和国治安管理处罚法》中打击网络违法犯罪的主要条款；《中华人民共和国电子签名法》、《刑法》中关于网络与信息安全的主要条款 |
| 信息安全技术 | 第三部分： 信息安全基础技术 | 识记 | 明文、密文、密钥、加密和解密等密码学基本概念和术语；对称密码体制的基本概念和典型算法；非对称密码体制的概念和典型算法；哈希函数的基本概念和术语；混合加密模式的工作原理；数字签名的概念；身份认证的基本方法；数字证书的作用与内容；认证中心（CA）的功能；公钥基础设施（PKI）的概念和组成；访问控制基本概念及三要素；安全审计的作用与功能 |
| 领会 | 加密解密模型；对称密码体制的优缺点；非对称密码体制的优缺点；哈希函数的特点；数字签名的工作原理；哈希函数、数字签名的应用；访问控制常用方法 |
| 应用 | 典型密码体制与数字签名的应用举例；系统日志安全审计的操作 |
| 综合 | 哈希函数的应用 |
| 第四部分： 网络安全防护技术 | 识记 | TCP/IP 协议、超文本标记语、超文本传输协议、端口、域名系统、统一资源定位符等网络基础概念；IPSec 的概念和功能；SSL 的概念和功能；VPN 的概念和特点；防火墙的概念和主要功能；无线局域网的概念和特点；无线局域网的安全威胁 |
| 领会 | IPSec 的工作模式；常见网络攻击目的和手段，包括社会工程学攻击、网络嗅探、网络钓鱼、拒绝服务攻击和远程控制攻击；VPN 的主要应用，包括远程访问、内联网、外联网的工作方式；无线接入点安全管理方法，包括修改管理员密码、采用加密传输、禁用 DHCP 服务等。 |
| 综合 | 无线路由器的安全设置 |
| 第五部分： 操作系统安全防护技术 | 识记 | 漏洞的概念与安全威胁；漏洞扫描的实现手段；恶意代码和计算机病毒的概念；恶意代码的安全威胁；木马的特点、传播方式与危害；端口扫描的安全威胁和隐蔽手段；操作系统的概念与功能；补丁程序的作用 |
| 领会 | 漏洞产生的原因；终端防护软件的功能和作用；关闭不必要服务和端口，开启审核策略和密码策略等的安全防护策略方法 |
| 综合 | Windows 操作系统安全使用安全；个人防火墙配置 |
| 第六部分：应用安全 | 识记 | 网上金融交易中常见的安全防护措施；邮件地址欺骗、垃圾邮件、邮件病毒等电子邮件安全威胁；数据备份的概念；账户口令的常见安全威胁；账户口令设置的基本原则；终端访问服务器的方式和特点 |
| 领会 | 电子邮件工作流程；垃圾邮件过滤、邮件加密和签名等电子邮件安全防护手段；数据备份的重要性和常见手段；数据加密和签名的重要性 |
| 应用 | 数据恢复操作方法和要点；数据加密和签名的常见手段 |
| 综合 | 浏览器安全设置和安全使用方法；电子邮件客户端安全设置和安全使用方法 |
| 第七部分：移动智能终端安全防护 | 识记 | 移动智能终端的概念和分类；常见的智能终端手机操作系统；伪基站的概念和伪基站攻击威胁；二维码的概念和二维码扫描威胁；移动智能终端遗失的安全防范措施；移动智能终端的加密软件；手机病毒的概念和危害；恶意扣费软件的安全威胁 |
| 领会 | 伪基站的工作原理；手机病毒的防范措施；二维码扫描的安全防范措施 |
| 应用 | 手机终端防护软件的设置 |
| 信息安全管理 | 第八部分： 信息安全管理 | 识记 | 信息安全管理的概念和内容；信息安全风险的概念；风险管理的概念和作用；风险评估的概念与作用；信息安全事件的概念与分级；信息安全事件分级考虑的要素；信息安全应急响应的概念和作用；灾难恢复的概念与作用；灾难备份的概念与作用；本地备份与异地备份的概念；数据级灾备和系统级灾备的概念；完全备份和不完全备份的概念 |
| 领会 | 成功实施信息安全管理的关键因素；信息安全应急响应管理过程；灾难备份方法 |

**附件2.3 长城网络靶场竞技系统考核大纲**

|  |
| --- |
| 一、基础理论题考核范围  1.包含基本编码、MySQL数据库安全、SQL注入利用、信息隐藏、XSS与编码、MSSQL数据库安全、MD5算法、缓冲区溢出之shellcode提取、移动应用的安全防护、逆向工程等内容；  2.包含主机恶意代码防护、网络单元信息的收集、暴力破解、Web入侵安全防护、安全设备与工具、系统压缩文件密码破解、代码审计等内容。 |
| 二、夺旗闯关题范围  1.包括WEB安全、密码学、安全杂项、逆向工程、溢出等5大类型题。  2.web安全方面包含文件包含(本地和远程)，文件上传和各种检查绕过和解析漏洞，php代码审计中的变量覆盖，命令执行，反序列化等漏洞和hash函数的不当使用等；  3.密码学包含古典密码中单表代换加密：凯撒密码 ，多表代换加密，以及其他类型加密如JSFuck，培根密码，栅栏密码，RSA加密，选择密文攻击，hash长度扩展攻击、DSA数字签名，以及伪随机数生成相关攻击；  4.包含安全杂项包括Morse 编码、格雷编码、曼彻斯特编码、XXencoding、Base64、ASCII 编码、以及条形码、二维码相关技术。包含元数据提取，像素值转化，png图片的lsb信息隐藏，图片长宽调整隐藏，gif图片多帧、时间轴中隐藏信息；pcap文件修复，http，dns等各种协议分析；压缩包暴力破解，明文攻击，伪加密；音频隐写： mp3 、 波形、频谱、LSB音频隐写；Ext，Fat等文件格式分析，内存数据分析等内容；  5.包含逆向工程包括脱壳技术、反调试技术、Linux逆向技术、python smali java 等语言的逆向技术，含windows PE 、 Linux ELF 文件的逆向内容。 |
| 三、主机渗透题范围  1.包含mailpress RCE漏洞、弱口令漏洞、权限提升、注入漏洞、失效的身份认证、安全配置错误、目录遍历漏洞、任意文件读取漏洞、后台密码爆破、认证绕过漏洞、网页编辑器漏洞、任意文件上传漏洞、敏感文件泄露漏洞、上传绕过漏洞、自定义页面上传木马、中间件解析漏洞等漏洞内容；  2.包括信息收集、php-fpm未授权访问、redis未授权访问、Web入侵安全防护、主机入侵与防护、数据库攻击与防护、溢出攻击、提权攻击与防护、后门技术与防护措施、操作系统漏洞等漏洞类型；  3.包含系统压缩文件密码破解、代码审计、密码哈希破解等内容。 |
| 四、攻防对抗范围  1.包含mailpress RCE漏洞、弱口令漏洞、注入漏洞、权限提升、失效的身份认证、安全配置错误、php-fpm未授权访问、中间件解析漏洞、目录遍历漏洞、爆破密码、认证绕过漏洞、任意文件上传漏洞、上传绕过漏洞、自定义页面上传木马等漏洞内容；  2.包含密码破解、主机入侵与防护、SQL注入、XXE实体注入、LDAP注入、OS命令注入、文件包含、代码注入、数据库远程登录、源码分析、欺骗技术、组件安全、提权攻击与防护、编码解码等内容。 |
| 五、取证溯源题范围  1.包含子域名爆破、伪造邮件、c段扫描、awvs扫描网站、爆破后台、sql注入、sqlmap扫描、编辑网站模板写shell、数据库下载、反弹内网shell等内容；  2.包含文件上传、xss、系统口令爆破、ftp爆破、ssh口令爆破、web口令爆破、mysql数据库密码爆破、sqlserver数据库密码爆破、vnc密码爆破等内容；  3.包含wordpress网站、dedecms网站、drupal网站、joomla网站、discuz网站、phpcms网站等内容；  4.包含wwwscan的使用、子域名爆破、awvs的使用、php木马的使用、c段扫描工具的使用、nslook的使用、使用ftp提权、撞库攻击、iTop系统的使用等内容；  5.包含远程命令流量识别、爆破流量识别、ftp流量识别、mysql协议识别、反序列化力量识别、weblogic后门识别、jsp木马识别、redis流量识别、arp流量识别、mail协议分析等内容；  6.包含pam后门查找分析、分析bash\_history、查找隐藏webshell、查找系统后门、计划任务后门分析等内容。 |

**附件3信息安全拔尖班面试考核问答模板**

1. 你觉得如何学好网络安全？谈谈你的规划？
2. 你了解的信息安全的威胁有哪些？
3. 在信息安全的道路上，你未来的职业规划？
4. 网络安全与网络空间安全的区别与联系？
5. 学习和掌握信息安全技能有什么意义？
6. 如果你是拔尖班的一员，你能为拔尖班的建设做什么或者打算做什么？（比如微信公众号运营、CTF平台建设、拔尖班的宣传、例会建设、网络安全实验平台建设）
7. 你是否能够在毕业之前一直坚持在实验室进行学习？是否能在毕业之前长期坚持学习信息安全？
8. 为了加入信息安全拔尖班，你做了哪些准备？
9. 学习网络安全你将会面临很多问题，比如方向迷茫，专业知识很难，你该怎么办？
10. 你认为自己在过去做了哪些有意义的事情（不局限于专业技能）。
11. 你有哪些方面比较擅长？如写作能力，web渗透或其他方面。
12. 谈谈你对网络安全的了解？如果有确定好的要走的方向，请说说你为什么要走这个方向？
13. 谈谈你对信息安全竞赛的认识？
14. 你觉得社会需要什么样的信息安全人才？
15. 谈谈信息安全与计算机其它专业的区别与联系？
16. 谈谈在没有老师带领你学网络安全的情况下，你该怎么办？