CSD 方向《网络安全》课程大纲

计算机网络是现代社会数字化、网络化和信息化的基础。与电力系统、通信系统一样，计算机网络日益成为支撑现代社会整体运行的基础设施。离开了计算机网络，人们的生产和生活将无法想象。但是，长期以来人们越来越清醒地认识到，计算机网络宛如一把高悬于人类头顶上的达摩克利斯之剑。人类社会对计算机网络的依赖程度越高，计算机网络的潜在威胁也就越大，网络安全的重要性亦随之愈加突显。网络安全是网络技术中一个永恒的主题。

就目前阶段而言，无论国际还是国内，网络安全问题都已然上升到国家安全的战略高度。拥有自主研发的网络安全技术，发展独立自主的网络安全产业，建立自主可控的网络安全体系，无论对哪个国家而言，都是关系到社会稳定和国家安全的重大问题。支撑和服务我国信息社会、信息产业的网络安全产品与服务的核心技术必须掌握在我国的技术专家手中。这是事关国家安全、社会稳定、产业健康发展的重要保障。

随着计算机系统和国际互联网的应用和普及，全社会对网络的依赖程度只会越来越高，对网络安全的需求也会随之越来越大，而具备网络安全知识和技能的高层次人才，必将成为整个信息产业竞相追逐的对象，这也就为掌握相关技术的有志青年提供了无比广阔的发展空间和数不胜数的就业机会。因此，学习和掌握网络安全技术对于提高相关专业毕业生的就业竞争力，相关领域工程技术人员的职场竞争力，乃至普通民众在未来社会的生存竞争力都是十分有益的。

鉴于以上原因，本方向结合自身的专业学科特点，拟开设为期 10 天的《网络安全》课程，具体包括：

- 网络安全概述
- 网络协议栈
- 对称密钥
- 公钥密码
- 消息摘要
- 嗅探器

- 安全 Web 服务器
- 端口扫描
- 网络诱骗
- 入侵检测
- 防火墙
- 内核加固
- 垃圾邮件过滤
- 恶意代码检测

等，共计 14 个专题。内容涵盖了当前网络安全研发的主要领域和方向，同时兼顾了技术的先进性和前瞻性。为了提高学员的动手实操能力，课程中还贯穿了 12 个实训案例：

- 基于 DES 加密的 TCP 聊天室
- 基于 RSA 算法的密钥分发
- 基于 MD5 算法的文件摘要
- 基于 Raw Socket 的网络嗅探器
- 基于 OpenSSL 的安全 Web 服务器
- 网络端口扫描器
- 网络诱骗系统
- 训练并测试用于入侵检测的聚类模型
- 基于 Netfilter 的防火墙内核扩展
- 提升系统内核抵御 TCP SYN 攻击的能力
- 基于 Sendmail 的垃圾邮件过滤器
- 基于 Clam AntiVirus 的恶意代码检测器

每个实训案例之前有知识讲解，之后有扩展提高，既讲理论，又重实践，立足现实，放眼未来。本课程的内容设计，无论是初入江湖的职场小白、还是呼风唤雨的技术大牛，都能从中受益。以下是本课程教学大纲：

网络安全概述 (0.25 天)	网络安全	网络安全与社会安全
		网络安全与信息安全
		网络安全与网络技术
		网络安全与密码科学

		网络安全与国家安全
	网络威胁	网络威胁的发展趋势
		网络威胁的主要特点
	研究范围	安全体系
		网络攻击
		安全防护
		防毒杀毒
		电子取证
		持续规划
		密码科学
		应用技术
	人员需求	网络安全人员的迫切性
		网络安全人员的稀缺性
	课程简介	网络协议栈
		对称密钥
		公钥密码
		消息摘要
		嗅探器
		安全 Web 服务器
		端口扫描
		网络诱骗
		入侵检测
		防火墙
		内核加固
		垃圾邮件过滤
		恶意代码检测
网络协议栈 (0.75 天)	Linux 网络协议栈	设计特点
		固定模式
		主要模块
	Linux 报文收发流	报文表示
		报文发送
		报文接收
对称密钥 (0.5 天)	知识讲解	DES 算法的历史
		DES 算法的特点
		DES 算法的内容
		TCP 协议
		套接字
		基本通信函数
	实训案例	基于 DES 加密的 TCP 聊天室
	扩展提高	DES 算法的安全性
		AES 算法
		高级通信函数
公钥密码	知识讲解	公钥密码的概念

(0.5 天)		公钥密码的特点
		RSA 算法的原理
		RSA 密钥的生成
	实训案例	基于 RSA 算法的密钥分发
	扩展提高	RSA 算法的安全性
		其它公钥密码
		多路 I/O
		异步 I/O
消息摘要 (0.5 天)	知识讲解	MD5 算法的特点
		MD5 算法的内容
	实训案例	基于 MD5 算法的文件摘要
	扩展提高	Linux 口令与 MD5 算法
		GRUB 口令与 MD5 算法
		字典攻击与 MD5 变换算法
嗅探器 (0.5 天)	知识讲解	原始套接字
		TCP/IP 协议栈
		数据封装与解析
	实训案例	基于 Raw Socket 的网络嗅探器
	扩展提高	通过 libpcap 库捕获数据包
		通过 tcpdump 命令捕获数据包
安全 Web 服务器 (0.5 天)	知识讲解	SSL 协议
		OpenSSL 库
		BIO 结构
	实训案例	基于 OpenSSL 的安全 Web 服务器
	扩展提高	客户端认证
		基于 IPSec 的安全通信
端口扫描 (0.5 天)	知识讲解	ICMP 扫描
		TCP 扫描
		UDP 扫描
		通过原始套接字发送数据包
	实训案例	网络端口扫描器
	扩展提高	扩展 ICMP 扫描
		扩展 TCP 扫描
		漏洞扫描
		基于 Nmap 的网络探测和安全审计
网络诱骗 (1 天)	知识讲解	网络诱骗系统的手段
		网络诱骗系统的分类
		可加载内核模块
		系统调用的本质
		截获键盘输入
	实训案例	网络诱骗系统
	扩展提高	截获键盘输入的其它方法
		启动时自动加载可加载内核模块

		隐藏可加载内核模块
		隐藏文件
		隐藏通信
		网络诱骗的发展趋势
入侵检测 (1 天)	知识讲解	KDD Cup 1999 数据集
		K-Means 聚类算法
		K-Means 聚类算法的缺陷与扩展
	实训案例	训练并测试用于入侵检测的聚类模型
	扩展提高	聚类精度对入侵检测模型性能的影响
		常用入侵检测工具
防火墙 (1 天)	知识讲解	什么是防火墙
		Netfilter
		IPTables
		Netfilter 内核扩展
	实训案例	基于 Netfilter 的防火墙内核扩展
	扩展提高	iptables 命令
		iptables 参数
		iptables 应用
内核加固 (1 天)	知识讲解	拒绝服务攻击
		僵尸网络
		内核代码剖析
	实训案例	提升系统内核抵御 TCP SYN 攻击的能力
	扩展提高	其它拒绝服务攻击
		基于 TCP SYN Cookie 的 SYN Flood 防御策略
垃圾邮件过滤 (1 天)	知识讲解	电子邮件的传输过程
		邮件传递的三个阶段
		SMTP 协议
		邮件报文格式
		POP3 与 IMAP 协议
		Sendmail 服务
	实训案例	基于 Sendmail 的垃圾邮件过滤器
	扩展提高	朴素贝叶斯算法
		词频逆文档频率
		垃圾邮件分类器
		机器学习的优势
恶意代码检测 (1 天)	知识讲解	什么是恶意代码
		可执行文件格式
		恶意代码检测技术与发展趋势
		Clam AntiVirus 工具包
	实训案例	基于 Clam AntiVirus 的恶意代码检测器
	扩展提高	使用 Clam AntiVirus 扫描电子邮件
		基于可信计算的恶意代码主动防御

本课程共 10 天，要求学员完成如下先修课程：

- 《C/C++程序设计语言》
- 《UNIX/Linux 系统高级编程》