附件 3

CISP 课程安排

时间	课程名称	课程内容
第一天	信息安全保障基础与实践	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。
	信息安全工程原理与实践	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	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）
	密码学应用	VPN 技术；PKI/CA 系统
第三天	网络协议及架构安全	TCP/IP 协议安全；无线安全/移动通信安全；网络架构安全
	网络安全技术	防火墙技术；入侵检测技术；其他网络安全技术
第四天	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
	安全攻防	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；计算机取证

第五天	操作系统及应用安全	操作系统基础/安全机制；Unix 安全实践；Windows 安全实践；数据库基础知识及安全机制/数据库管理系统安全管理/中间件安全；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
	信息安全法制研究与标准	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；等级保护标准
第六天	访问控制与审计监控、软件安全开发	访问控制模型；访问控制技术；审计和监控技术；软件安全开发概况；软件安全开发的关键阶段
	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
	信息安全管理基础	信息安全管理基本概念;风险管理的概念和作用;安全管理控制措施的概念和作用;信息安全管理方法
第七天	信息安全管理措施	安全基本管理措施
	重要安全管理过程	信息安全管理体系
第八天	串讲	
	CISP 考试	100 道单项选择题，两小时