网络信息安全

课程目标：

本课程将全面介绍现有网络信息安全防范措施，以网络协议的发展为主线，结合病毒的发展过程来综合分析。在分析工具上，将介绍多种网络监测工具、常用分析软件安，注重理论与实践相结合，每介绍一种类型安全攻防，均以实例阐述。

通过对本课程的学习，使学生掌握网络安全技术的安全问题、加密技术、防火墙技术、 VPN 技术、入侵检测与预警技术、防病毒技术、拒绝服务攻击、欺骗攻击、常见的系统漏洞等安全方面的内容。

适用学员：

企业信息安全主管，参与信息系统审计和管理体系规划的人员，提供信息安全咨询服务的专业人员，其他对信息安全全面的知识体系感兴趣的人员。具体培训对象包括：

- 企业信息安全主管
- 信息安全业内人士
- IT 或安全顾问人员
- IT 审计人员
- 安全设备厂商或服务提供商
- 信息安全类讲师或培训人员
- 信息安全事件调查人员
- 其他从事与信息安全相关工作的人员（如系统管理员、程序员、保安人员等）

课程设计：

授课课时:	2 天
授课条件：	学员必须具有基本的计算机操作知识
内容摘要：	**一、网络安全对策** 了解 IP 报头、TCP 头格式、TCP 传输原理，理解 IP 欺骗的原理，了解信任关系、TCP 序列号预测、使被信任主机丧失工作能力的一般方法、序列号取样和猜测方法及 IP 欺骗的防止。理解防火墙概念，采用防火墙的必要性，知道防火墙的构成、网络政策、包过滤。 **二、网络安全分析和安全策略**

理解网络安全基础知识和含义，知道计算机安全的正式分级、网络安全模型结构、安全服务的层次配置、网络安全的安全策略，了解网络安全技术现状，知道 Internet 上的危险和安全缺陷、因特网不安全的原因、TCP/IP 协议的安全缺陷、TCP/IP 协议常见的攻击方式。理解 TCP/IP 协议各层的安全性，掌握信息安全技术与网络安全，知道信息安全模型与主要技术、信息安全系统设计原则，会信息安全系统的设计与实现。

三、Unix 系统安全

了解 Unix 网络不安全的因素，知道特权软件的安全漏洞、特洛伊木马的原理，理解 Unix 系统安全的基本概念、用户的安全、程序员的安全性的设置。知道 Unix 系统的安全措施、 文件系统安全、X Windows 的安全性和网络安全措施。

四、Windows 系统安全

理解 Windows 2000 环境配置、安全机制、安全模型，知道 Windows 2000 已知的安全漏洞、如登录验证机制漏洞、浏览器安全漏洞、IGMP 安全漏洞等。

五、Web 系统安全

了解 Web 结构、会配置 Web 服务器、Web 浏览器、通用网关接口(CGI)、cookies，知道 Web 安全性的框架及如何实施 Web 安全框架。了解 CGI 脚本的安全性、Cookies 的安全性和 Java 的安全性。

六、加密与认证技术

了解密码学的基本概念，理解分组密码和序列密码的原理，知道公钥密码体制和常规信息加密技术，掌握对称密钥加密体制、非对称密钥加密体制及数字签名方法，知道 RSA 公钥体制、DES

加密算法，知道信息认证技术、消息认证、身份认证、数字签名的概念。

七、防火墙设计

了解防火墙基础知识、防火墙模型与安全策略、防火墙的主要组成部分、防火墙的缺陷、防火墙结构、双重宿主主机的概念及服务方式、知道堡垒主机基础知识、基本原则，会配置和保护堡垒主机，会进行堡垒主机的维护，知道防火墙测试的基本方法。

八、网络安全扫描工具

知道扫描工具的工作原理，了解 ISS 的功能，会安装使用 SATAN 软件包及其他扫描工具，掌握端口扫描中的一些技巧。

九、网络监听及审计监测工具

了解网络监听基本知识、知道网络监听定义和网络监听的作用，会系统本身提供的一些工具和常用网络监听工具及检测和分析工具。

十、欺骗攻击

了解常见的欺骗攻击的方法，如 IP 欺骗、Web 欺骗以及 DNS 欺骗。知道它们的欺骗原理以及预防方法。

十一、计算机病毒

了解计算机病毒的特征、分类、破坏行为以及作用原理，对几种常见病毒的源代码进行分析，知道计算机病毒的预防和清除方法。

十二、Intranet 与 VPN

了解 Intranet 网络安全结构，知道 Intranet 基本概念、Intranet 解决方案的基本结构、Intranet 系统目标及任

	务、Intranet 的网络逻辑构成、Intranet 网络拓扑结构。掌握虚拟专用网(VPN)技术、基于 PC 防火墙的 VPN 设计。
授课语言：	中文