TREND MICRO

趋势科技认证信息安全专员(TCSP)教材

网络安全与病毒防范

趋势科技网络（中国）有限公司／编

- 黑客盛行，病毒泛滥……
- 在网络世界里如何才能确保自己安全地生存?
- 本书带你走进“神圣”的网络安全大门，从此你也是“行家里手”！

上海交通大学出版社

趋势科技认证信息安全专员(TCSP)教材

网络安全与病毒防范

趋势科技网络(中国)有限公司　编

上海交通大学出版社

内 容 提 要

本书是TCSE初级认证课程的培训教材，全书共分三篇。第一篇：网络安全基础，就当前网络安全的现状进行了分析，并就常见的网络安全防范技术和产品展开了描述，同时阐述了构建企业安全网络的过程和策略，以帮助初学者轻松跨入网络安全领域的大门，对于长期从事网络安全工作的人士也将大有裨益；第二篇：病毒、恶意代码和垃圾邮件，深入阐述了病毒的相关知识，所谓知己知彼，百战不殆，通过这部分内容的学习，读者能够全面了解病毒的特征和应对方法；第三篇：趋势科技防毒战略，为用户分析了当前企业防毒技术的现状，给用户带来了企业防毒领域最先进的安全防护策略，帮助用户建立最新的防毒观念。

图书在版编目(CIP)数据

网络安全与病毒防范/趋势科技网络(中国)有限公司编. —上海:上海交通大学出版社,2004

ISBN7-313-03665-5

Ⅰ.网… Ⅱ.趋… Ⅲ.①计算机网络-安全技术②计算机病毒-防治 Ⅳ.①TP393.08②TP309.5

中国版本图书馆CIP数据核字(2004)第019245号

网络安全与病毒防范

趋势科技网络(中国)有限公司 编

上海交通大学出版社出版发行

(上海市番禺路877号 邮政编码200030)

电话:64071208 出版人:张天蔚

上海锦佳装璜印刷发展公司 印刷 全国新华书店经销

开本:787mm×1092mm 1/16 印张:14.75 字数:354千字

2004年4月第1版 2004年4月第1次印刷

印数:1—5050

ISBN7-313-03665-5/TP·586 定价:26.00元

序一

我们正生活在一个网络时代，这是一个激动人心的时代，计算机网络技术的发展改变了人类所熟悉的生活形态与方式，电子邮件、WWW 服务、网上购物、在线娱乐等应用使得地球变得越来越小了，企业的发展也越来越依靠信息化作为助动力。但应该看到的是，随之而来的越来越多的安全隐患，网络攻击事件和病毒事件已经成为社会关注的焦点。面对日益复杂的黑客以及病毒攻击事件，架构一个全方位完整的防护体系已刻不容缓。这些工作需要专业的技术咨询服务和专业人员进行处理。于是，网络安全服务和网络安全人才成为了社会一大迫切的需求。

作为网络防毒与互联网内容安全软件及服务领域的全球领导者，趋势科技不仅以卓越的前瞻和技术革新能力提供优秀的安全产品，更注重为企业提供高品质的服务。同时，趋势科技视构筑安全的网络环境为己任，通过建立完善的教育培训体系，将怎样构筑安全有效的网络专业知识、最先进的病毒防范理念和技术提供给迫切需要的人士，帮助那些有志从事或正在从事网络安全工作的人士进一步提升网络安全知识，帮助企业培养迫切需要的网络安全人才是我们的一个重要目标。

趋势科技已经开始逐步在全国建立多家授权培训中心体系，通过与优秀的培训机构以及高等院校合作，推广趋势科技的 TCSE 认证。另外，通过已经开展并将一直持续的“病毒防范知识普及校园行活动”普及网络安全知识，为网络信息安全教育事业贡献一份力量。

趋势科技网络（中国）

总经理　吕理臣

2004 年 3 月

序二

现今网络环境越来越复杂，网络入侵的危险性越来越大，特别是2003年的冲击波病毒，对全球众多电脑都造成了冲击，危害有目共睹。而每次病毒事件到来之所以能造成巨大的损失，都和计算机网络使用者安全意识薄弱以及安全知识匮乏有关。因此，掌握必要的病毒防范技术和网络安全知识是计算机使用者一项基本技能。企业更加关注黑客与病毒攻击带来的严重后果，在很多的企业中甚至设置了专门的网络安全相关职位，专业的网络安全职位渐已成为 IT 行业最热门的职位。

对专业的网络安全人才的培养已经引起了广泛的关注，很多知名的大学已经设置了信息安全专业，CIW、CISSP 等非厂商中立性认证以及防火墙、入侵检测等安全厂商提供的技术认证越来越被众人所推崇。随着网络病毒的越发频繁地扰乱，反病毒技术已经向多层次、整体化发展，这就涉及如何在企业内构建完整的防毒体系问题。

作为防病毒领域领先厂商趋势科技开始逐步推广的 TCSE 认证培训及时地满足了广大企业的需求。通过与高等院校的合作，趋势科技直接将网络安全知识带给求知若渴的学生，以满足学子们对网络安全知识的需求，并将进一步促进网络安全知识在校园的普及。

国家八六三计划信息安全主题专家
上海交通大学信息安全工程学院副院长、教授
李建华

2004 年 3 月

前　言

面对现今网络环境越来越复杂、网络入侵的危险性越来越多的现状，对于网络信息安全与防毒观念您是否一知半解？对于企业的防毒工程建置是否一筹莫展？完善的信息系统需建立在“安全”的机制上，通过信息安全专家有系统的课程培训与技术认证，可以让用户在IT信息领域中建立“铁三角”的信息安全防护网；同时，也可以提升本身安全防护的价值。

作为防病毒及内容安全软件服务领域的全球领导者，趋势科技以卓越的前瞻和技术革新能力引导了从桌面防毒到网络服务器和网关防毒的潮流，同时也愿意将提高广大计算机网络使用者的安全意识和防范水平视作己任，趋势科技的信息安全专家认证课程就是针对这一需求开发的。

本书是TCSE初级认证课程的培训教材，全书共分三篇。第一篇：网络安全基础，就当前网络安全的现状进行了分析，并就常见的网络安全防范技术和产品展开了描述，同时阐述了构建企业安全网络的过程和策略，以帮助初学者轻松跨入网络安全领域的大门，对于长期从事网络安全工作的人士也将大有裨益；第二篇：病毒、恶意代码和垃圾邮件，深入阐述了病毒的相关知识，所谓知己知彼，百战不殆，通过这部分内容的学习，读者能够全面了解病毒的特征和应对方法；第三篇：趋势科技防毒战略，为用户分析了当前企业防毒技术的现状，给用户带来了企业防毒领域最先进的安全防护策略，帮助用户建立最新的防毒观念。

本书由趋势科技总部资深网络安全专家组成的培训团队组织开发，由几位在国内长期从事网络安全咨询和培训工作的专任培训讲师编辑成书。全书由马宜兴负责总编，陆亚灵、徐白负责整理和校稿，趋势科技中国服务事业部经理Kevin Chai对全书进行了审阅。

希望本书的出版能为广大有志从事网络安全事业或对网络安全感兴趣的人提供一些有益的帮助。

编　者

2004年2月

目录

第一篇　网络安全基础

第二篇 病毒、恶意代码和垃圾邮件

第三篇 趋势科技防毒战略

第一篇

网络安全基础

第 1 章　网络安全概述

本章概要

本章介绍网络安全的定义、安全网络的基本特征以及计算机网络面临的威胁。本章内容包含以下几部分：

- 网络安全的定义；
- 安全网络的基本特征；
- 计算机网络面临的威胁。

课程目标

通过本章的学习，读者应能够：

- 了解网络安全的定义及其涵盖的范围；
- 了解计算机网络面临的威胁主要来自哪些方面；
- 了解安全的计算机网络的基本特征。

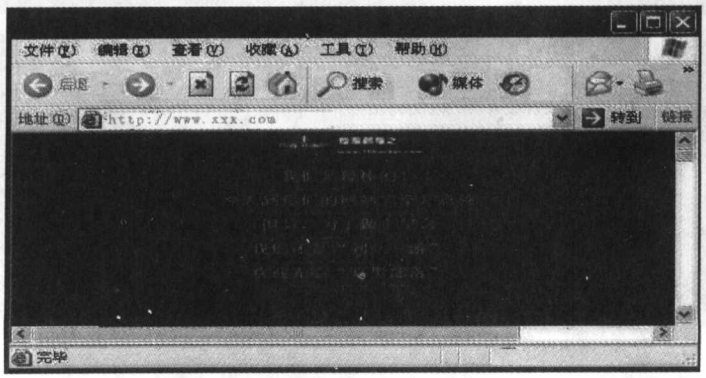
1.1　网络安全的背景

在我们的生活中，经常可以见到下面的报道：

- XX 计算机系统受到攻击，造成客户数据丢失；
- XX 网站受到黑客攻击；
- 目前又出现 XX 计算机病毒，已扩散到各大洲；
- ……

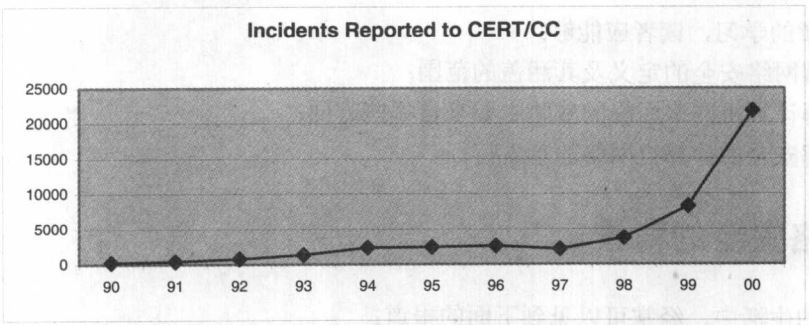
计算机网络在带给我们便利的同时已经体现出了它的脆弱性……

❑ 经常有网站遭受黑客攻击



❑ 用户数据的汇漏

❑ 网络攻击事件与日俱增



❑ 网络病毒在全球范围内迅速扩散

随着数字技术及 Internet 技术的日益发展，病毒技术也在不断地发展和提高。它们的传播途径越来越广，传播速度越来越快，造成的危害越来越大，几乎到了令人防不胜防的地步。

下面两张图分别为某天的两个不同时间点的病毒扩散情况，通过比较可以看出网络病毒的扩散速度是极快的。