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（第四版）

趋势科技(中国)有限公司/组编
马宜兴/主编

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

(第四版)

主　编　马宜兴
编　写　张海峰
　　张志徐

上海交通大学出版社

内 容 提 要

本书是TCSE认证课程系列培训教材，全书围绕企业目前遇到的两大安全威胁——黑客与病毒展开论述，详细地描述了黑客攻击原理和计算机病毒基本原理，深入阐述了应对信息安全威胁的防御措施，对常见的信息安全技术与产品作了概括性介绍，同时对企业如何有效构建完整的安全防护体系提供了参考建议。本书还对计算机病毒的攻击方法、危害与影响、发展趋势和防护策略作了权威的论述，同时介绍了业界最新的病毒防护理念。

本书既适用于普通本科院校、高职高专院校计算机及相关专业的学生，又是初学者轻松跨入信息安全领域的钥匙，也是专业信息安全人士的有效参考书籍。

图书在版编目（CIP）数据

网络安全与病毒防范 / 马宜兴主编.—4版.上海：
上海交通大学出版社，2009
趋势科技认证信息安全专员（TCSP）教材
ISBN 978-7-313-03665-0

Ⅰ. 网… Ⅱ.马… Ⅲ.①计算机网络－安全技术－技术培训－教材
②计算机病毒－防治－技术培训－教材 Ⅳ.TP393.08 TP309.5

中国版本图书馆CIP数据核字（2009）第149757号

网络安全与病毒防范
（第四版）
马宜兴 主编
上海交通大学出版社出版发行
（上海市番禺路951号 邮政编码 200030）
电话：64071208 出版人：韩建民
常熟文化印刷有限公司印刷 全国新华书店经销
开本：787mm×1092mm 1/16 印张：16 字数：399千字
2004年4月第1版 2009年8月第4版 2009年8月第9次印刷
印数：36401－41431
ISBN 978-7-313-03665-0/TP 定价：36.00元

序一：时间与我们的行业

今天是4月5日，2009年第一季度刚刚结束，从洛杉矶飞往南京的航班上，我看了一部名叫《返老还童》(Benjamin Button)的电影。这部电影让我想起上周，也就是2009年4月1日爆发的Conficker（或称Downad）病毒，还有早先于1992年3月6日发现的著名病毒——米开朗基罗！我喜欢看电影，因为电影能以短短两小时的如梭光影浓缩百味杂陈的漫漫人生，也能让我体验数百年的沧海桑田！

这部电影根据小说《本杰明·巴顿奇事》改编而来，故事描写了一个出生时老态龙钟的奇异男婴随着一天天长大而越变越年轻，最终回到婴儿状态。整个影片都在讲述时间的魔力…… 在我看来，时间是人世间最神秘莫测的存在方式，哪怕人类的时钟只倒拨一秒，这个世界都会天翻地覆、乾坤逆转……

当然，我写这篇博客并不是为了介绍一部好看的电影，我只是想和大家分享自己对这个行业的感悟——这就是我们所从事的内容安全行业…… 我从事这一行已20余年了。这20余年既是个时间概念，也代表了这个行业的整个发展历程和兴衰起伏。

4月1日，新闻媒体铺天盖地地报道了一种实施恶意行为的“恐怖”病毒，称这种病毒将大举袭击因特网和成千上万台电脑——这就是叫做Conficker/Downad的病毒。

整个情形让我想起了1992年3月6日米开朗基罗病毒爆发之时的情景。那时候，人们还没有将“反病毒”视为一个行业，而是把它看成是一些怪人用来“耍酷”的谈资或软件工具。米开朗基罗病毒病毒是在1991年4月于新西兰首次发现，病毒设定在1992年3月6日发作，届时所有受感染电脑的整个磁盘将全部被格式化。将其命名为米开朗基罗病毒是因为3月6日正是伟大的艺术家——米开朗基罗的生辰。距3月6日还剩两周左右时，许多报章杂志和电视新闻都开始报道这种病毒，大范围的恐慌不断蔓延，很多普通人也第一次认识了“计算机病毒”这种东西。1992年3月6日，当“世界末日”真正来临时，全世界范围内却只报告了10000到20000例数据丢失事件。有些人说这只是危言耸听的炒作，开始把反病毒业叫做“骗子”行业。虽然米开朗基罗病毒的“宣传”确实有些言过其实，但经历了另外几次类似的病毒事件之后，人们终于清醒地意识到，数字格式的数据确实会受到恶意代码的破坏，而后来的事实则充分证明了反病毒行业存在的必要性。

时间推移到上周——情况如出一辙：Conficker/Downad病毒成了媒体和公众谈论的焦点，恶意软件研究人员（包括趋势科技员工）有理由认为，这种结构复杂的多面性蠕虫病毒已经感染了500多万台电脑；到4月1日当天，“蠕虫大师”应该会发布一个命令来唤醒成千上万受到感染的僵尸电脑，利用它们来作乱滋事！但4月1日发

生的真实情况却并非如此。不过我们都明白，这只能说明蠕虫大师决定多等些时候再发动攻击，或者是想避免大张旗鼓。同时，他们也可能打算以隐蔽的方式长期利用这些僵尸机来窃取信息、发动本地化 DDoS 攻击抑或通过出租病毒来获利。

米开朗基罗病毒和 Downad 病毒的爆发时间相隔 18 年之久。但前后比照，就仿佛看到了历史重演。这是又一次“炒作”还是反病毒行业新浪潮的开端？

这也引发了我对反恶意软件行业生命周期的思考。反病毒行业似乎永远不会“衰老”，甚至永远无法彻底跨越从起步到成长之间的鸿沟。每当我们以为自己已经走出这个怪圈，新一轮的威胁便迫使整个行业投入新的战斗，让我们重新走进生命周期的轮回：最初满怀梦想，然后得到早期用户的认可，当我们以为渡过了鸿沟期时，新的威胁类型再次到来——一切就好像《返老还童》里的故事，我们这个行业也和电影主人公一样在一天天变年轻。

有时候，我也会怀疑这种“永远年轻”的概念是否永远适用于反病毒行业，但是，每当我们以为反恶意软件终于实现了“商品化”时，历史就又会重演，病毒威胁一次又一次将我们打回原形，我们就要一次次地经历学习、成长和挑战自我的过程。Conficker 或者 Downad 病毒让人们多少意识到了现实状况：问题根本还没解决，事实上仍在不断扩散和日益恶化，目前的解决方案显然并未奏效。18 年过去了，如今的数字世界承担着更大的风险，因为各种至关重要的信息和经营活动都更加依赖数字网络了。

我们从事的是一个永远不老的产业。这就意味着反病毒领域始终存在着不断创新变革的空间和必要，我们还要时时刻刻关注网络环境，了解最关键问题所在，从而为应对下一轮威胁准备最为有效的解决方案。只要耽搁一秒，就会造成重大影响。放眼反病毒行业目前的环境，我目睹了种种新动态和新趋势——云计算正在兴起、病毒威胁的形势瞬息万变，而顾客的购买行为也正向 SaaS（软件即服务）模式发展……

18 年前，客户端发现了米开朗基罗病毒，当时的我们迈入了服务器领域的幼稚期，而现在，我们又处在了客户端-云端的幼稚期。就像《返老还童》这个故事一样，反病毒行业仿佛生来就是越变越年轻的“还童”之身，虽然这似乎与行业生命周期理论的传统观点背道而驰，但我们这些从业者仍要为此而坚定履行自己的使命和战略。内容安全行业（或者说反病毒威胁行业）依然很年轻，仍然需要广开思路、大力创新，同时也要具备勇于尝试全新解决方案的出众胆识。

趋势科技 CEO

Eva Chen

（注：本文摘自 Eva 的 Blog，2009.4.5）

序二：投身到安全技术的潮流中

非常高兴看到这样一本优秀著作的再版。我一直关注技术，尤其是网络安全领域技术的新发展、新趋势。随着全球经济的发展，越来越多的企业，感受到了趋势科技所带来的改变，感受到了网络安全技术对企业的价值。

实际上，站在这样一个时间点上，世界经济正经历着惊涛骇浪，亚太地区作为新兴市场，在全球经济链条上的作用日益明显，也就因此更会承受全球经济带来的各种影响。随着网络的发展，信息化进程的加快，网络安全已经在世界范围内，成为衡量一家企业发展能力的重要指标，亚太区的经济增长近年来持续强劲，企业大多数面临管理升级、信息化升级的关键阶段，趋势科技也因此迎来了一个高速增长的机遇。在这个特殊的时代背景下，大中型企业网络安全市场一直是趋势科技的优势所在，过去一年中，趋势科技致力为大中型企业用户提供完善的网络安全解决方案，这也恰恰顺应了这个时代。中国古话：“顺势而为”，相信是任何企业、任何个人成长的一种智慧。

近年来在国际网络安全领域，高频率、大破坏力的病毒爆发，安全危机事件确实层出不穷，这在技术上对安全服务提供商提出了非常高的要求。网络安全技术，作为IT技术中的高阶应用，在攻防两端都需要高技术人才的支撑。防守（Defend）是我们通常能够理解的防止病毒进入、防止爆发、防止损失等，而进攻（Attack）则强调了病毒爆发后迅速、安全的查杀，对企业的优质服务贯穿其中，这就是网络安全服务的价值链所在。在中国，趋势科技已经在近期向媒体和公众展示了最新产品技术 TDA 和全新的病毒防护架构——“云安全”技术，在亚太其他国家和地区，趋势科技都相应推出了适合本地企业发展状况、技术环境的最新技术产品。相信在趋势科技强大技术团队的支持下，技术与用户需求紧密结合，大型企业用户的网络安全防范将跨越一个新的台阶。

作为一家国际化的企业，全球范围内的安全领域优秀人才，都是趋势科技最为看重的宝贵财富，实际上这是一个隐形的战场，世界范围内的技术高手都不断投入其中，趋势科技创立的 20 年历史中，每一次技术革新带来的喜悦都成为趋势科技成长的动力，同样也成为世界范围内我们客户企业的安全保障。作为亚太区总裁，我由衷地希望中国、印度、新加坡等各个新兴市场国家的技术人才加入趋势科技，或投身进当前时代安全技术的潮流中，成为企业及个人价值的创造者、享有者。

趋势科技全球执行副总裁
亚太区总裁
Oscar Chang

序三：时代需要网络安全人才

现今网络环境越来越复杂，网络入侵的危险性越来越大，像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。而每次病毒事件的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。

目前，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的扰乱，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部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

再版前言

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意识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，全书涵盖内容十分广泛。第 1~8 章对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 9~14 章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；最后，本书还专门用 1 章的篇幅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——“云安全”技术，帮助读者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。第四版在之前版本的基础上增加了网页挂马、手机病毒等流行病毒的趋势分析。趋势科技资深病毒专家张志徐带领的中国区网络安全监测实验室的反病毒专家和著名信息安全专家张海峰先生分别就病毒技术和黑客攻防部分作了修改，增加了技术深度。全书由马宜兴任主编，趋势科技中国服务事业部经理蔡昇钦对全书进行了审阅。

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士提供一些有益的帮助。

本书的编写得到了上海交通大学出版社的大力支持，在此表示感谢！

由于时间仓促，谬误之处还请广大学员和读者指正，如有疑问，可发送电子邮件到以下信箱：tcse@trendmicro.com.cn。

祝大家能愉快地学习，并顺利地通过趋势科技信息安全专家认证。

编　者

2009 年 6 月

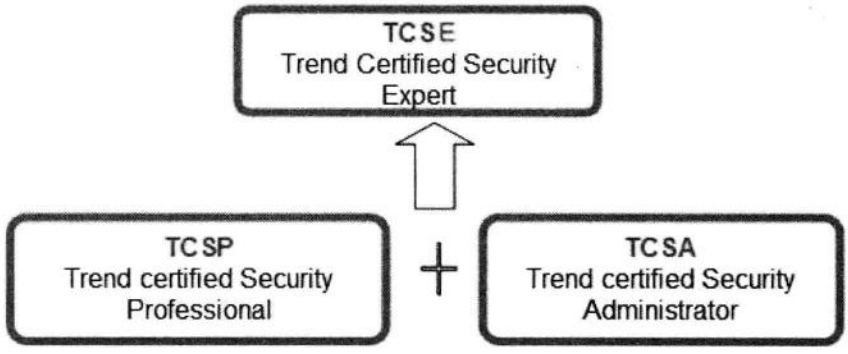
TCSE 认证之路

TCSE 简介

TCSE（Trend Certified Security Expert，趋势科技认证信息安全专家）是趋势科技为应对当前越来越复杂的网络环境而推出的一项国际性认证，取得 TCSE 资质即代表着具备了业界最顶尖的防病毒、安全技能。趋势科技公司希望通过 TCSE 课程的训练与认识，将如何“如何构建有效的防毒环境”这项专业技能提供给现在紧缺的现代信息专业人才。

TCSE 认证之路

TCSE 共分为两个阶段：TCSP（Trendmicro Certified Security Professional，趋势科技认证信息安全专员）、TCSA（Trendmicro Certified Security Administrator，趋势科技认证信息安全管理员）。具备了 TCSP 和 TCSA 资质后，可以直接申请 TCSE 认证资格。



TCSE 课程内容

TCSP	趋势认证信息安全专员(Trend Certified Security Professional)
课程说明	主要内容：全面了解基本的网络弱点，了解安全技术原理，了解业界新技术，了解各类安全技术的产品及其实现方式，了解内容安全（防病毒）的难度及在网络安全中日益重要的地位
TCSA	趋势认证信息安全企业网络管理员 (Trend Certified Security Administrator)
课程内容介绍	1. OSCE (防毒墙网络版) 2. IMSA (InterScan Messaging Security Appliance) 3. IWSA (InterScan Web Security Appliance) 4. TMCM (中央控管) 5. NVWE (网络病毒墙)
教材	趋势科技原版教材

* 更多更新的信息可登录趋势科技网站：http://cn.trendmicro.com/cn/support/techsupport/tcse/index.html

如何报名？

趋势科技在全国各地设有授权培训中心，您可登录趋势科技网站进行查询，也欢迎来电咨询。

查询网址：http://cn.trendmicro.com/cn/support/techsupport/tcse/partner/index.html

咨询电话：021－63848899

邮　　箱：tcse@trendmicro.com.cn

课 程 综 述

课程内容

本课程以分析计算机网络面临的安全威胁为起点，阐述了常用的网络安全技术，首先介绍主流网络安全产品和常用网络安全策略，并着重强调内容安全（防病毒）在网络安全中的重要地位。随后，着重介绍病毒及与病毒防护相关的知识，并就目前业界最先进的病毒防护理念展开了深入的说明。

本课程的内容分为两个部分，涉及以下几个方面：

- 计算机网络面临的安全威胁；
- 常用的计算机网络安全技术；
- 主要的网络安全产品类型；
- 企业网络安全策略；
- 病毒、恶意代码与垃圾邮件的基础知识；
- 计算机病毒的危害与防范措施；
- 病毒的发展趋势；
- 传统病毒防范技术的不足；
- 趋势科技企业防护战略。

课程目标

本课程的目标是提高学员的网络安全意识和病毒防范水平，使学员熟悉基本的网络安全理论知识和常用网络安全产品，了解部署整个网络安全的防护系统和策略的方法，尤其是病毒防护的相关策略。在此基础上，让学员充分了解病毒防范的重要性和艰巨性，了解“内部人员的不当使用”和“病毒”是整个网络系统中最难对付的两类安全问题。

主要涉及以下内容：

- 基本的网络弱点；
- 安全技术原理；
- 各类安全技术的产品及其实现方式；
- 内容安全（防病毒）的难度及在网络安全中日益重要的地位；
- 病毒防范技术和病毒防护体系的实施。

授课对象

本课程面向下列人员：

- IT 部门工作人员；
- 工程师；
- 对网络安全基础知识有兴趣的人士。

目　　录

第1章　信息安全概述

本章概要

- 信息安全威胁；
- 信息安全弱点；
- 信息安全定义；
- 安全网络基本特征；
- 信息安全体系结构；
- 操作系统的安全级别。

1.1　信息安全背景

1.1.1　信息安全事件大事记

在我们的生活中，经常可以见到下面的报道：

- ××计算机系统受到攻击，造成客户数据丢失；
- ××网站受到黑客攻击；
- 目前又出现××计算机病毒，已扩散到各大洲；
- 手机越来越成为黑客攻击的对象；
- ARP 病毒几乎使得公司网络瘫痪；
- ……

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……

2008 年，美国东海岸连锁超市(East Coast)的母公司 Hannaford Bros.称，该超市的用户数据库系统遭到黑客入侵，造成 400 多万张银行卡的账户信息泄露，因此，导致了 1800 起与银行卡有关的欺诈事件。

2007 年，“ARP 欺骗”病毒肆虐，国内某著名高校百余宿舍网络端口被封，只因内网有电脑感染此病毒，导致所有用户受网页挂马攻击。

2006 年，“熊猫烧香”病毒造成了国内几百万用户感染。

2005 年，美国超过 300 万的信用卡用户资料外泄，导致用户财产损失，同时国内众多金融机构先后成为黑客们模仿的对象，设计了类似的网页，通过网络钓鱼的形式获取非法利益。

2004 年 4 月 30 日，震荡波（Sasser）病毒首次被发现，短短一个星期时间之内就感染了全球 1800 万台电脑，成为当年当之无愧的“毒王”。