高职高专计算机任务驱动模式教材

计算机网络安全

冯　昊　编著

清华大学出版社

高职高专计算机任务驱动模式教材

计算机网络安全

吴一编著

清华大学出版社
北京

内 容 简 介

本书结合作者多年的实际网络安全管理和教学经验，采取以能力为本位，先了解黑客的攻击技术，再做网管的编写思路，通过具体的网络安全案例，介绍了计算机网络安全、网络攻击与入侵、通信子网安全防范、网络服务器与主机的安全防范、病毒与木马的安全防范、电子商务的安全、计算机网络安全管理等实用内容，并配有大量习题和实训操作。

本书可作为高职高专计算机类相关专业的网络安全教材，也可作为网络安全的培训教材。

图书在版编目(CIP)数据

计算机网络安全/冯昊编著. —北京：清华大学出版社，2011.8(2014.2 重印)
(高职高专计算机任务驱动模式教材)
ISBN 978-7-302-25637-3

Ⅰ. ①计… Ⅱ. ①冯… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 099503 号

责任编辑：张　景　束传政
责任校对：李　梅
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：16.25　　**字　　数**：390 千字
版　　次：2011 年 8 月第 1 版　　**印　　次**：2014 年 2 月第2 次印刷
印　　数：4001～4500
定　　价：28.00 元

产品编号：037617-01

丛书编委会

出版说明

我国高职高专教育经过近十年的发展，已经转向深度教学改革阶段。教育部2006年12月发布了教高[2006]16号文件“关于全面提高高等职业教育教学质量的若干意见”，大力推行工学结合，突出实践能力培养，全面提高高职高专教学质量。

清华大学出版社为了进一步推动高职高专计算机专业教材的建设工作，适应高职高专院校计算机类人才培养的发展趋势，根据教高[2006]16号文件的精神，2007年秋季开始了切合新一轮教学改革的教材建设工作。

目前国内高职高专院校计算机网络与软件专业的教材品种繁多，但切合国家计算机网络与软件技术专业领域技能型紧缺人才培养培训方案并符合企业的实际需要、能够成体系的教材还不成熟。

我们组织国内对计算机网络和软件人才培养模式有研究并且有实践经验的高职高专院校，进行了较长时间的研讨和调研，遴选出一批富有工程实践经验和教学经验的双师型教师，合力编写了这套适用于高职高专计算机网络、软件专业的教材。

本套教材的编写方法是以任务驱动案例教学为核心，以项目开发为主线。我们研究分析了国内外先进职业教育的培训模式、教学方法和教材特色，消化吸收优秀的经验和成果。以培养技术应用型人才为目标，以企业对人才的需要为依据，把软件工程和项目管理的思想完全融入教材体系，将基本技能培养和主流技术相结合，课程设置中重点突出、主辅分明、结构合理、衔接紧凑。教材侧重培养学生的实战操作能力，学、思、练相结合，旨在通过项目实践，增强学生的职业能力，使知识从书本中释放并转化为专业技能。

一、教材编写思想

本套教材以案例为中心，以技能培养为目标，围绕开发项目所用到的知识点进行讲解，对某些知识点附上相关的例题，以帮助读者理解，进而将知识转变为技能。

考虑到是以“项目设计”为核心组织教学，所以在每一学期配有相应的实训课程及项目开发手册，要求学生在教师的指导下，能整合本学期所学的知识内容，相互协作，综合应用该学期的知识进行项目开发。同时在教材中采用了大量的案例，这些案例紧密地结合教材中的各个知识点，循序渐进，由浅入深，在整体上体现了内容主导、实例解析，以点带面的模式，配合课程

后期以项目设计贯穿教学内容的教学模式。

软件开发技术具有种类繁多、更新速度快的特点。本套教材在介绍软件开发主流技术的同时，帮助学生建立软件相关技术的横向及纵向的关系，培养学生综合应用所学知识的能力。

二、丛书特色

本系列教材体现目前的工学结合教改思想，充分结合教改现状，突出项目面向教学和任务驱动模式教学改革成果，打造立体化精品教材。

(1) 参照或吸纳国内外优秀计算机网络、软件专业教材的编写思想，采用本土化的实际项目或者任务，以保证其有更强的实用性，并与理论内容有很强的关联性。

(2) 准确把握高职高专软件专业人才的培养目标和特点。

(3) 充分调查研究国内软件企业，确定了基于 Java 和. net 的两个主流技术路线，再将其组合成相应的课程链。

(4) 教材通过一个个的教学任务或者教学项目，在做中学，在学中做，以及边学边做，重点突出技能培养。在突出技能培养的同时，还介绍解决思路和方法，培养学生未来在就业岗位上的终身学习能力。

(5) 借鉴或采用项目驱动的教学方法和考核制度，突出计算机网络、软件人才培训的先进性、工具性、实践性和应用性。

(6) 以案例为中心，以能力培养为目标，并以实际工作的例子引入概念，符合学生的认知规律。语言简洁明了、清晰易懂、更具人性化。

(7) 符合国家计算机网络、软件人才的培养目标；采用引入知识点、讲述知识点、强化知识点、应用知识点、综合知识点的模式，由浅入深地展开对技术内容的讲述。

(8) 为了便于教师授课和学生学习，清华大学出版社正在建设本套教材的教学服务资源。在清华大学出版社网站(www. tup. com. cn)免费提供教材的电子课件、案例库等资源。

高职高专教育正处于新一轮教学深度改革时期，从专业设置、课程体系建设到教材建设，依然是新课题。希望各高职高专院校在教学实践中积极提出意见和建议，并及时反馈给我们。清华大学出版社将对已出版的教材不断地修订、完善，提高教材质量，完善教材服务体系，为我国的高职高专教育继续出版优秀的高质量的教材。

清华大学出版社

高职高专计算机任务驱动模式教材编审委员会

rawstone@126. com

前　言

随着计算机网络的日益普及和广泛应用，网络和信息的安全问题日益突出，构建安全、可靠、健康的网络应用环境，维护国家信息网络的安全和保障敏感信息资料的安全，已成为社会信息化进程中亟待解决的问题，为此，完善信息安全立法，学习掌握网络安全防范技能，着力加强网络安全队伍建设和安全技术研究，培养网络安全专业人员，对保障网络和信息的安全，提高国家网络安全水平，就显得至关重要和紧迫。

计算机网络安全是一门比较传统和经典的课程，目前国内与计算机网络安全相关的教材，在数量和种类上都较多，但真正编写得比较实用的教材却不多。计算机网络安全涉及的专业知识面较广较深，需要具备较丰富的网络安全管理和攻防实战经验，要真正写好确实不容易。

本书以网络安全理论知识够用、实用，突出网络安全实用技能培养，以能力为本位作为编写指导思想。采取先了解黑客的攻击技术，再做网管的编写思路来组织全书的内容和章节顺序。

本书的编写目标是通过对该教材内容的学习和实践操作，培养具有独立承担大、中型网络的安全设置与防范和安全管理的能力，成为一名合格的计算机网络安全专业人员。

本书的特色主要体现在以下三个方面。

(1) 内容新颖，实用性和可操作性强，攻防案例真实有效。在内容上做到与时俱进，紧扣时代特色，针对目前主流的网络服务器操作系统，详细介绍网络攻击与入侵、网络和服务器的安全防范技术和电子商务安全的整体解决方案。

(2) 突出网络安全实用技能培养，以能力为本位作为编写的指导思想。

(3) 在内容的组织和讲解上，充分体现“易学易教”的原则。

本书还详细全面地介绍了电子商务的安全知识和电子商务安全的整体解决方案，同时还详细介绍了利用 PGP 加解密软件，实现对邮件通信、数据存储和传输的高强度加密保护。最后，针对电子商务应用常用的安全 Web 服务器，详细介绍了安全 Web 服务器的安装、配置与使用方法，因此，本书也可作为电子商务专业的电子商务安全教材。

本书配有习题和实训操作，相关资源可访问作者网站来获得，网址是 http://www.pcnetedu.com/getbkres.asp。全书共 7 章，建议学时数不低于 64 学时。

限于笔者学识，疏漏之处，敬请批评指正。

作　者

2011 年 4 月

目 录

第 1 章　计算机网络安全概述

本章主要介绍计算机网络安全的概念、计算机网络的安全现状和面临的安全威胁，计算机网络安全的要素与解决途径，以及我国的信息安全法律、法规。

1.1　计算机网络安全的概念

计算机网络由网络硬件设备、网络控制管理协议与软件，以及网络存储和传输交换的网络数据三部分构成，因此计算机网络安全包括物理安全和信息安全两个方面。

物理安全主要指网络系统的设备及相关设施受到物理保护（防火、防盗、防雷、防静电、机房温度湿度控制保护、电压控制保护和通信线路安全等），免于破坏和丢失，并提供设备正常运行所需的工作环境。

通常情况下，计算机网络安全主要指计算机网络的信息安全。计算机网络的信息安全包括网络通信协议、各种网络服务和操作系统软件、网络存储处理和传输交换的网络数据的安全等方面。网络存储的数据包括服务器、终端用户主机以及网络存储设备中存储的数据。网络存储设备主要有磁盘阵列柜、IP SAN 和 FC SAN 等。

国际标准化组织（ISO）将“计算机安全”定义为：为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然的原因和恶意而遭到破坏、更改和泄露。计算机网络安全包含计算机安全，二者有着密切的关系，因此，计算机网络安全可定义为：计算机网络系统中的硬件、软件及其数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改和泄露，保障网络系统连续可靠地正常运行，网络服务不被中断。

计算机网络安全的目标是通过采用各种技术和管理措施，使网络系统和各项网络服务正常运行，经过网络传输和交换的数据不会发生丢失、篡改或泄密，从而确保网络的可靠性，网络数据的机密性、完整性和可用性。

1.2　计算机网络安全现状与安全威胁

1.2.1　计算机网络安全现状

计算机网络是计算机技术和通信技术发展的必然产物，进入 20 世纪 90 年代以后，以因特网为代表的计算机网络得到了飞速发展，加速了全球数字化、网络化和信息化革命的

进程。

近年来，互联网在我国得到了持续的快速发展，已成为重要的国家基础设施，在国民经济建设中发挥着日益重要的作用。据中国互联网络信息中心（CNNIC）在 2010 年 7 月 15 日发布的《第 26 次中国互联网络发展状况统计报告》，截至 2010 年 6 月底，我国网民规模已达 4.2 亿，互联网普及率进一步提升，达到 31.8%。

随着我国互联网普及率的逐年提高，互联网已走进人们的工作与生活，影响和改变着人们的生活、工作和学习方式。互联网丰富的信息资源给用户带来了极大的方便，由于因特网是一个开放的、超越组织与国界的、不安全的互联网络，这就给上网用户和数据信息带来了极大的安全隐患。计算机信息的安全问题，尤其是计算机网络的信息安全问题正变得日益突出。

随着海关、税务、电力、金融等基础性行业信息化的深入，网络安全已成为关系到国家安全和社会稳定的重要因素。目前，网络安全形势不容乐观。木马与病毒传播相当泛滥，网络攻击事件时有发生，网络钓鱼（Phishing）欺诈在全世界范围内变得非常猖獗，数量急剧攀升。利用伪装成中国银行或中国工商银行网站的恶意网站进行诈骗钱财的事件，已让人们感受到网络钓鱼已不再遥远。

钓鱼网站由于投入少、回报大，伴随网购热潮已经悄然兴起。据国际行业组织反钓鱼工作组的数据，2009 年一个月新建的独立钓鱼网站就高达 5 万个。截至 2009 年 11 月底，中国反钓鱼网站联盟累计收到的钓鱼网站投诉达 12000 例，钓鱼网站投诉前三位的分别是淘宝网、CCTV 和腾讯网，占投诉总量的 74%以上。

网络钓鱼主要利用障眼法和贪图便宜的心理来实施诈骗。钓鱼网站主要集中在两方面：一种是模仿央视或其他抽奖网站，比如，仿冒央视的“非常 6+1”或春晚节目的中奖信息来骗取网民钱财，其主要特征是以中奖为诱饵，欺骗网民填写身份信息、银行账户等信息。另一种是仿冒淘宝网店、工商银行网站、中国银行网站等在线支付网页，然后诱骗用户访问这些钓鱼网站，从而骗取支付宝账户和支付密码、银行卡账户和密码，达到套取银行账户资金的目的。

钓鱼的银行网站除了在内容上与真实的银行网站模仿得相似之外，在网站的域名上，也会使用障眼法做得非常相似。比如，真正的工商银行网站域名为 www. icbc. com. cn，而钓鱼网站的域名则设计为 www. 1cbc. com. cn，二者的区别仅是小写字母 i 和数字 1 的不同。又比如中国银行网站的域名为 www. bank-of-china. com，钓鱼网站的域名则设计为 www. bank-off-china. com。

目前，黑客通过网络有组织地制作、传播和销售木马病毒的黑客产业链正在形成。据 360 安全卫士总裁齐向东称，2009 年中国黑客通过制作、传播和销售木马病毒的非法收入估计有 100 亿元以上，按照这个销售额来估计，从业人员可达 10 万人。这些木马病毒的大量制作和传播，给网络和信息安全带来了极大的安全威胁，严重妨碍了信息化社会的健康发展。同时，木马病毒攻陷入侵用户主机后，除了窃取机密信息外，该主机还可能成为受黑客控制的“僵尸电脑（俗称肉鸡）”，众多的“僵尸电脑”在网络中形成“僵尸网络”（BotNet），这些受黑客控制的“僵尸网络”，在利益的驱使下，可根据需要对要攻击的目标网站或目标网络发起大规模的分布式拒绝服务攻击（Distributed Denial of Service，DDoS），使被攻击的目标网站或目标网络瘫痪。“僵尸网络”是目前进行 DDoS 攻击的理想工具，这种攻击方式已经沦为进行不公平竞争或者网络恐怖主义示威和实施的工具，成为黑客最青睐的作案工具。

“僵尸网络”制造者的收入来源包括 DDoS 攻击、窃取机密信息(信用卡或银行卡账号、游戏账号和游戏装备、财务信息以及各种服务的密码等)、发送垃圾邮件、网络钓鱼、搜索引擎作弊、广告点击欺诈以及传播恶意软件和广告软件等,这些行为都是可盈利的,而且“僵尸网络”可以同时实施这些行为。据赛门铁克公司(Symantec)的统计,目前互联网中的垃圾邮件有 80%来自于僵尸网络。2010 年 2 月,微软公司成功游说美国司法部签发法院令,让 277 个与 Waledac 僵尸网络(每天可发送 15 亿条垃圾信息)相关的域名停止解析,从而迅速有效地切断了 Waledac 僵尸网络数以千计的链接。但微软公司的做法并不能完全解决僵尸网络的问题,仅仅是使 Waledac 僵尸网络的问题得到暂时的缓解。

因此,采取有效措施,构建安全、可靠、健康的网络应用环境,维护国家信息网络的安全,已成为社会信息化进程中亟待解决的问题,为此,完善信息安全立法,着力加强网络安全队伍建设和技术研究,培养网络安全专业人员,就显得至关重要和紧迫。

1.2.2　计算机网络面临的安全威胁

计算机网络面临的安全威胁是多方面的,有人为原因,也有非人为原因,其安全威胁主要表现在以下方面。

1. 计算机网络自身特性所带来的安全威胁

计算机网络的开放性、自由性和国际互联特性,使计算机网络面临的攻击是多方面的,网络安全威胁面临国际化挑战。

对计算机网络的攻击可来自物理传输线路,也可来自对网络通信协议的攻击,或通过计算机软件或硬件的漏洞来实施攻击。计算机网络的国际互联特性,使攻击者可以是本国或本地用户,也可以来自全球任何国家。

2. 计算机网络自身的缺陷所带来的安全威胁

(1) 计算机网络通信协议缺陷所带来的安全威胁

目前互联网广泛使用的是 TCP/IP 协议簇。这些协议在设计时由于考虑不周(在设计的当时,也可能不存在这方面的安全威胁)或受当时的环境所限,或多或少存在着一些设计缺陷。网络协议的缺陷是导致网络不安全的主要原因之一。

互联网协议在设计时不存在太多的安全问题,因此协议对安全问题考虑得较少。比如在 1983 年设计 DNS 的时候,不需要考虑安全问题,甚至到 1993 年(首款真正的浏览器 Netscape Navigator 诞生)都不存在这个问题。直到 20 世纪 90 年代末,人们才在安全上大量投入,也就是从那时起,开始有人盯上了网络中的资产并实施破坏。

由于安全是相对的,没有绝对的安全,因此,没有绝对安全可靠的网络通信协议。下面简要介绍几个网络通信协议缺陷所带来的安全威胁。

① TCP 协议缺陷易导致 SYN 泛洪攻击,服务器容易遭受拒绝服务或分布式拒绝服务攻击。

传输控制协议 TCP 提供了面向连接的、高可靠性的端到端的连接服务。TCP 协议在建立 TCP 连接之前的三次握手过程中存在缺陷,这种协议缺陷可导致 SYN 泛洪攻击(SYN Flood),使网络应用服务器易遭受到拒绝服务(Denial of Service,DoS)或分布式拒绝服务攻击(DDoS)。

下面对 TCP 协议在三次握手过程中存在的缺陷做简要分析。

在建立 TCP 连接时，服务请求方（客户端）向服务器（服务端）发起建立连接的请求报文（SYN 标志位置为 1）；服务器给客户端回应响应报文（ACK 和 SYN 标志位均置为 1）；客户端在收到服务方的响应报文后，正常情况下，客户端应给服务器回应一个响应报文（ACK 标志位置为 1），从而完成三次握手过程，建立起 TCP 连接。但此时，若客户端故意不回复第三次握手的 ACK 回应报文，这将使服务器为接收到该回应报文而等待一段时间，该等待时间为 SYN 超时时间（30s～2min）。

由于 TCP 连接已建立到中途，服务器端会为这个即将完成的 TCP 连接分配一定的系统资源，因此，这种处于半连接状态的 TCP 连接，会消耗一定的服务器资源。

如果一个客户端或大量的客户端（比如僵尸网络）同时向服务器发起建立大量的半连接，则会很快消耗尽服务器的系统资源，正常的应用服务进程（比如 Web 服务、FTP 服务或邮件服务等）因无法获得可用的系统资源而被中止，导致服务器无法为正常的客户提供服务，最终导致服务器出现拒绝服务的现象。

② TLS 和 SSL 协议的漏洞易导致用户浏览器被劫持，遭受到中间人攻击。

PhoneFactor 公司的 Marsh Ray 和 Steve Dispensa 安全专家于 2009 年 11 月 4 日正式公开了 Marsh Ray 于 2009 年 8 月份发现的 TLS 和 SSL 协议中的一个致命安全漏洞。攻击者可以利用这种漏洞劫持用户的浏览器，并伪装成合法用户，进行中间人攻击（Man in The Middle）。

这两位安全专家指出，由于 TLS 协议中验证服务器及客户机身份的一连串动作中存在前后不连贯的问题，这就给攻击者可乘之机。TLS 协议中存在的这种漏洞在 SSL 协议上同样存在。TLS 和 SSL 协议中的该漏洞，给攻击者发起 HTTPS 攻击也提供了便利。

传输层保密协议 TLS（Transport Layer Security）和 Socket 层保密协议 SSL（Secure Sockets Layer）是目前广泛使用的安全保密协议，也是互联网的标准通信协议。互联网中的加密通信广泛采用了 TLS 或 SSL 协议来进行。目前网络银行、网上在线交易和数字证书的加密传输均采用 HTTPS 协议，而 HTTPS 协议是 HTTP 协议和 TLS/SSL 协议的集合体，HTTPS 协议中的加密部分采用的是 TLS 或 SSL 协议。因此，TLS 和 SSL 协议的该漏洞对互联网业的安全影响是全面的和致命的。

发现这一漏洞之后，Marsh Ray 和 Steve Dispensa 很快将其报告给了互联网安全促进行业联盟（ICASI），该联盟由思科、IBM、Intel、Juniper、微软和诺基亚共同创立。同时还报告给了 Internet 工程任务组（IETF）以及几家开源的 SSL 项目组织。2009 年 9 月 29 日，这些团体经过讨论后决定推出一项名为 Mogul 的计划，该计划将负责修补这个漏洞，计划的首要任务是尽快推出新的协议扩展版，以修复该漏洞。

目前微软的所有 Windows 版本（包括服务器和客户端产品）均受此安全漏洞影响，微软表示，当前还没有发现有利用此漏洞进行的攻击行为，由于该漏洞影响的是互联网标准，因此微软不是单一受害者。

③ DNS 漏洞导致域名解析被劫持，带来严重的安全威胁。

在 1983 年设计 DNS 时，未考虑安全问题，导致 DNS 系统的安全漏洞一直较多。2008 年初，IOActive 公司的安全研究人员 Dan Kaminsky 在同多个 DNS 系统商共同开发安全补丁的时候，发现了 DNS 系统的一个结构性的、非常严重的安全漏洞。利用该漏洞，攻击者只需利用一个有效的漏洞脚本，就能在 10 秒之内发起一个“DNS cache poisoning”（DNS 缓存投

毒)攻击,该攻击成功后可向 DNS 服务器的缓存插入任何数据,比如将错误的域名解析指向信息注入到 DNS 服务器缓存,从而改变域名的解析结果,导致受到污染(投毒)的 DNS 服务器对外提供错误的域名解析,达到劫持 DNS 域名解析,将访问者在不知情的情况下引导到黑客指定的恶意网站(比如钓鱼网站、木马自动下载网站或者黑客事先设计好的其他网站)的目的,因此,该漏洞的危险性极高,利用该漏洞可造成域名劫持攻击,使攻击者能轻松地伪造任何网站,使用户浏览到伪造的网站,邮件也可能被发送到错误的地方,给全球用户带来一系列严重的安全威胁。

DNS 是互联网的一项核心服务,相当于整个互联网的心脏,DNS 解析的准确性非常重要,一旦遭到破坏,互联网的正常运转将被打乱。为了不让互联网遭受重创,Dan Kaminsky 坚持在该漏洞得到解决之前不透露漏洞的细节。

发现该安全漏洞后,Dan Kaminsky 立即联系了 ISC 公司的总裁 Paul Vixie(BIND 的设计者,BIND 是 Linux/UNIX 平台的 DNS 服务软件),告之了漏洞细节。之后,DNS 业界的思科、微软、ISC 等互联网域名解析服务软件厂商开始共同研究和商谈漏洞的修复问题,并最终推出了由多家厂商共同开发的 DNS 漏洞修复补丁。

为了让网络运营商知道这个漏洞和漏洞的严重性,说服网络运营商和 DNS 服务器拥有者升级 DNS 系统,Dan Kaminsky 于 2008 年 7 月 8 日公开了该漏洞及其危害性,但未透露漏洞的细节。2008 年 7 月 9 日,思科、微软、ISC 等互联网域名解析服务软件厂商纷纷发布了关于该漏洞的安全公告,要求 DNS 服务商升级 DNS 系统。由于该漏洞影响的面非常广、非常严重,该漏洞公布后,轰动了整个 IT 界,该漏洞被称为 Kaminsky 漏洞。Dan Kaminsky 近照如图 1.1 所示。

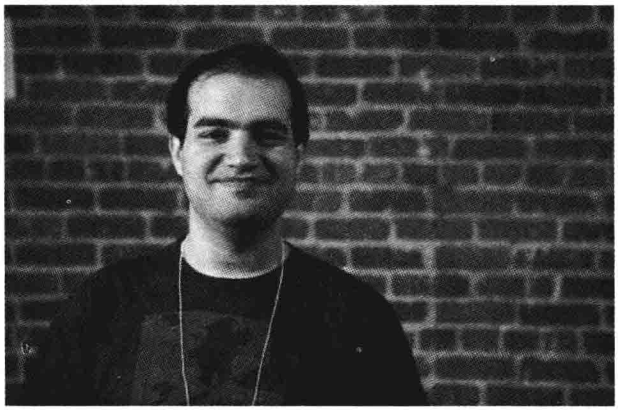

图 1.1　DNS 严重安全漏洞发现者 Dan Kaminsky

之后不久,Matasano 安全公司的一个员工在其博客中泄露了该漏洞的细节。为此,Dan Kaminsky 在其博客上发表了一个紧急消息,提醒 DNS 漏洞细节被泄露,攻击即将开始。2008 年 7 月 22 日,针对该漏洞的探测程序被发布,7 月 23 日,针对该漏洞的完整攻击程序被发布,并随后广泛流传。

目前,Kaminsky 漏洞细节在黑客界已众所周知。下面对该漏洞的细节和攻击原理作简要分析,以帮助读者更好的理解漏洞对于安全威胁的严重性。

首先介绍一下 DNS 查询是如何进行的。客户机在通过域名访问网站时,将首先触发一