黑客防线

防黑反毒技术指南

郝文化　主编

机械工业出版社
CHINA MACHINE PRESS

黑客防线

防黑反毒技术指南

郝文化　主编

机 械 工 业 出 版 社

本书采用实例解析的方法讲述了网络安全及其防范知识。本书共分12章，主要针对Windows环境下的网络安全的机理，维护步骤和方法，常见病毒的防范与清除措施以及对网络安全构成极大威胁的黑客攻击行为，应采取的安全防范措施进行全面地阐述。

全书实例丰富，语言通俗，叙述深入浅出，实用性强。既可作为大中专院校计算机专业的教学和参考用书，也可作为各类计算机安全培训班的培训教材，还可作为广大的网络爱好者、网络管理员的学习和参考用书。

图书在版编目（CIP）数据

防黑反毒技术指南/郝文化主编 .—北京：机械工业出版社，2004.1
（黑客防线）
ISBN 7-111-13140-1

Ⅰ.防… Ⅱ.郝… Ⅲ.①计算机网络—安全技术 ②计算机病毒—防治 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2003）第087067号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）
策划编辑：胡毓坚
责任编辑：周艳娟
责任印制：路 琳
北京蓝海印刷有限公司印刷·新华书店北京发行所发行

2004年1月第1版·第1次印刷
787mm×1092mm 1/16· 25印张·615千字
0001—5000册
定价：37.00元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话：（010）68993821、88379646
封面无防伪标均为盗版

出版说明

近年来，计算机网络在国内得到了迅速的发展。在网络的大量应用中，安全正面临着前所未有的挑战。信息安全已经成为一个综合的工程，甚至将成为一门新兴的研究学科，需要我们在网络安全领域进行长期的研究和攻关。

网络的基础在于资源的共享，这一直是网络的基本准则。随着 Internet 的飞速发展，网络上的资源共享越来越强化。随之而来的，网络安全问题也越来越突出了。网络在带给人们诸多便利的同时，也成了许多犯罪分子攻击的目标。他们以计算机为工具，同时又以计算机为目标，在网上对计算机数据信息进行恶意的修改、删除，从而造成计算机系统难以正常运行甚至瘫痪。如果我们从另一方面去看问题，黑客也使我们发现自己网络的缺陷并改进它，从某种意义上说，日益完善的安全系统和逐渐完美的防火墙，是和黑客技术密不可分的。黑客的存在是网络发展的必然结果，尤其在我国，互联网络还处于雏形阶段，存在着不可忽视的缺陷与漏洞。如何改良网络结构，完善网络安全体系，是我们的当务之急。政府部门也对网络信息安全非常重视，并鼓励大力发展信息安全事业，以使我国在全球信息网络化的发展中占据主动地位。

目前，社会上对精通网络与信息安全知识的人才需求越来越强烈，广大技术人员和网络用户也十分希望能迅速提高自己应对安全问题的能力。由此，机械工业出版社联合北京地海森波网络技术有限公司《黑客防线》编辑部共同策划出版了“黑客防线”丛书，旨在为读者提供有关网络安全方面的知识和技术，从不同侧面阐述网络安全的相关技术。在丛书撰写过程中，切实考虑读者对知识的需求，内容做到通俗易懂，其中涉及的很多技术都是工作在网络安全第一线作者的心血结晶。对从事网络安全事业的技术人员来说，本套丛书是一个很好的帮手，从中可学到很多实用技术和宝贵经验，从而得心应手地应对各种网络安全问题。对于那些想学习网络安全知识和技术的读者而言，本套丛书也不失为好的学习工具书，通过学习不仅能迅速掌握网络安全知识，提高自身防范能力，而且为走上网络安全事业的道路奠定了基础。

我们始终坚持以普及网络安全知识，加强全民安全意识，提高我国信息技术和网络安全水平为己任，希望这套丛书的出版能满足读者的需求，并请广大读者批评指正，提出宝贵意见。

机械工业出版社

前　言

2003年年初，突如其来的“蠕虫王”病毒，给互联网造成的损失不亚于发生在美国的“9.11”恐怖袭击事件。“蠕虫王”病毒只有276个字节，该病毒利用Microsoft SQL Server的漏洞进行传播，由于Microsoft SQL Server在世界范围内的广泛普及，使得该病毒得到了广泛传播，从而对互联网造成了极大的损失。仅在中国就导致80%以上网民不能上网，很多企业的服务器因感染上此病毒而导致网络瘫痪。在美国、泰国、日本、韩国、马来西亚、菲律宾和印度等国家的互联网服务也受到严重影响。

“蠕虫王”病毒只是一小段具有自我复制性和传送性的程序，竟然导致了整个互联网服务的瘫痪，人类耗时近20年，花费数万亿美元建设的信息网络竟然如此不堪一击，这一事件的发生，又一次唤醒了人们必须重视网络安全。

在信息社会中对网络安全构成威胁的不仅仅来自无特定攻击目标的各类病毒，还包括针对特定攻击目标采取的各种攻击行为，即通常所说的黑客攻击。随着网络社会的到来，网络安全已成为制约其发展的瓶颈问题。切实保证广大计算机网络爱好者能够更好地利用网络资源，切实保证网络的安全，笔者经过认真收集素材和整理，组织业内资深人士编写了本书。

本书全面阐述了Windows环境下的网络安全机理、维护步骤和方法，针对对网络安全构成威胁的病毒传播方式和黑客攻击手段，全面介绍了应采取的各种安全防范措施。此外，本书还对黑客技术发展趋势(比如针对.NET漏洞的攻击防范)进行了分析，同时提供了相应的防范措施，供广大网络爱好者、计算机网络管理员参考。

本书的特点是：全面剖析了最新病毒的传播方式和最新黑客攻击手段，在此基础了介绍了相应的防范措施和解决方案。本书实例众多，且所举出的实例针对性强，分析透彻，突出体现了本书以实例为中心的特点。通过阅读本书，能加强读者的网络安全防范意识，提高维护网络安全的技能。

书中列出的实例程序源代码只是该程序的部分核心代码，读者若需完整的源代码，请与作者联系，E-mail：hwhpc@163.com。

特别注意的是，如果用户安装了瑞星、金山毒霸、Norton等杀毒软件，这些软件的系统实时防护功能可能会自动删除源代码文件、黑客工具软件，或者将这些文件移动到隔离区，从而导致源代码文件和黑客攻击软件无法使用。如果想查看到这些代码或者软件的运行结果，读者可以关闭这些软件的系统实时防护功能。

有些源代码或黑客工具可能会导致格式化硬盘，导致非法操作，向Internet发送密码，导致局域网病毒传播等恶劣后果，因此在使用这些代码和工具时必须采取相关措施，保护好自己的重要文件，本书源代码和介绍的黑客工具仅做研究和维护网络安全之用，请勿非法使用，否则后果自负。

本书语言通俗易懂，内容丰富，突出了以实例为中心的特点，适合广大Windows操作系统用户、网络爱好者、网络管理人员作为网络安全手册使用，同时也可供从事基于Windows网络安全的网络工程师参考。

本书由郝文化主编，焦苍、邓勋、王淳、杜庆丽、李治国、王晓寒等担任主要的编写工

作。参与本书编写的人员还有毛翔、王昆、颜治平、邓超、焦英芹、许海亮、曹发辉、焦国良、魏国伟、李想、张劲枫、王宝、吴圣贤、田园、代亚勇、黄新民、闫桂玲、贾旭东、蔡瑞仕、李高阳、李晓聪、李红敏、焦保良、王晓寒、干昆蓉、南琛、王莉莉、刘树年、翟进营、赵沛泽和逯颖等。在本书的编写过程中得到了刘青松、田茂敏、苏萍、李建康、周勤、顾舒的鼎立支持，在此对他们表示衷心感谢。

如果读者愿意参加“防黑反毒技术”的学习培训，或是在学习过程中发现问题，或有更好的建议，欢迎致电我们，我们非常愿意随时同熟悉防黑反毒的高手保持经常的联系。

由于编者水平有限，书中疏漏和错误之处，恳请读者批评指正。

编　者

目　录

第 1 章　计算机安全与黑客

知识点

- 计算机安全
- 黑客文化
- 计算机安全与黑客引发的思考

本章导读

全球信息网络的建设和发展，对整个社会的科学与技术、经济与文化带来了巨大的推动和冲击，同时也给网络的安全运行带来更多的挑战。

由于全球 Internet/Intranet 的发展及应用，使得 Internet/Intranet 安全面临重大的挑战。资源共享和信息安全是一对孪生矛盾。Internet/Intranet 的发展，使得资源共享进一步加强，因而安全问题也就更加地突出。一般认为，计算机网络系统的安全威胁主要来自黑客的攻击。黑客攻击早在主机终端时代就已经出现了，随着 Internet 的发展，现代的黑客转变为以网络攻击为主，攻击的手段更是千变万化。

1.1　PC 系统安全

1.1.1　计算机安全

什么是计算机安全？广义地讲，计算机安全是指防止其他人利用、借助自己的计算机或外围设备，做任何事情。当然，这一定义过于广泛，然而，这一定义却引出了不得不面临的一些极为重要的问题，这些问题是任何希望设置一种有效的安全机制的人都必须面对的。

通过对众多的黑客攻击事件的分析可以发现，黑客最感兴趣的是滥用主机标识，而不是过分触及个别主机中的专门资源，他们利用这些标识暗渡陈仓，向外连接其他可能更感兴趣的目标。但是，也有些人可能对个别计算机中的某些数据感兴趣，而不管它们是否是公司的敏感材料或政府机密。

通常对“什么是计算机安全”这一问题的答案是采取必要的计算机安全防范专用措施。存有敏感文件的计算机可要求额外的口令级别，或者甚至(在少数场合)对文件采取相应的加密措施。同样，如果感兴趣的目标计算机可以向外连接，管理人员可以设定需要具有一定特权的人才能访问该网络。如果可能，所有这些访问都应该通过一个后台守护程序(Daemon)来进行，它将执行额外的日志记录。

现在越来越多的人采用 Windows 2000/XP 及其以上版本的操作系统，在上网的同时，可能已经遭受黑客的攻击，而被攻击者却不能及时发觉。借助被攻击者的计算机，黑客可以达到任何不可告人的目的，而不承担相应的责任。

当然，任何人都想保护自己的计算机资源不被他人非法利用，在这种情况下，最有效的

办法是把攻击者拒之于门外，即首先不让他人非法进入自己的计算机系统，这是一种很好的方法。但是它是建立在系统安全问题来自外部攻击的假设条件下的。

在选择计算机安全的防范方法时，首先需要搞清的是“威胁到计算机系统安全的是谁?”，这样才能够建立起足以防范单个攻击的计算机系统，但在借助各种先进技术和设备进行攻击的情报部门面前，它却显得无能为力。对于前者，增强口令安全性即可解决计算机系统的安全问题，然而后者却能够、并且可能借助于搭线窃听和密码分析，监视别人的计算机和电缆的电子发射，甚至瞄准在计算机房的“暗箱操作”。保证单纯的计算机安全并不是目的，它只是达到保证信息安全这一目的的手段。计算机安全防范的强度与其所受的威胁成比例，其他防范措施虽已超出了本书的讨论范围，但同样必不可少。

在配置安全机制之前必须搞清楚的问题包括“能在安全保障方面付出多大代价?”，比如要保护的资料的价值为1000元，却花费2000元去保证其安全性，显然没有太大的实际意义。安全问题的解决的代价是直接的财政开支，诸如建立防火墙网关需要额外的路由器和计算机。虽然要在投资和安全机制之间寻求到绝对的平衡很难，但这是在配置安全机制时所追求的目标。

1.1.2 安全策略

安全策略(Security Policy)是安全决策的集合，它们集中体现了一个组织或个人对安全的态度。更准确地说，安全策略对于可接受的攻击行为，以及应对攻击行为做出何种响应，都有明确的界限。从本质上讲，安全策略对不同的组织或个人来说是有区别的。大学里一个系的安全需求不同于一个公司的产品开发部的需求，同样，后者又不同于一个军事部门的安全需求，显然对于个人来说系统安全又有所区别。但是，每个组织或个人，如果要求安全系统有预警功能，都应有一整套安全策略。

首先是决定“允许什么样的攻击行为”和“不允许什么样的攻击行为”。一些公司希望限制流出的信息，以防止雇员将公司有价值的数据泄漏出去。其他方面还受到技术方面的影响：某一特定协议尽管很有用处，由于不能安全地管理它，也不能采用。还有一些涉及到诸如雇员未经适当授权而进口软件之类的问题，公司并不希望由于侵害其他人的权利而被起诉。

安全策略中的关键是如何做好系统的安全防范，正如一个城堡，如果忽略了安全的防范，那么就会被敌人轻而易举地攻破；如果在这个城堡的防护方面尽了最大的努力，那么敌人就不会轻易得手。

如果不上网或者不与Internet连接，计算机安全应该不是问题，黑客绝对不会对没有物理连接的系统造成任何的威胁，但是在这个信息时代里，孤立是多么可怕。因此，我们不主张断开与大多数站点的连接。网络有很多优点，脱离网络则是自动放弃这些优点。也许脱离连接是一种正确的选择，但这是需要权衡风险与利益的关系后才能做出的决定。

根据上面的论述，我们有必要认真研究黑客的攻击手段，所谓“知己知彼、百战不殆”，这样能将安全风险降到最小，同时还提供大部分(并非全部)网络连接利益。对于众多的电脑用户及网络站点来说，应该积极地防范黑客攻击而不是被动地采取方法。

首先，任何程序，不管它看起来如何完美，但仍可能隐藏着安全漏洞(谁能料到，在某些计算机中，一个整数除法错误，竟然会导致系统崩溃!)。因此坚信，任何程序在被证明是无安全漏洞之前，均是有安全漏洞的。

进而言之，安全策略无论是否正式成文，都客观存在。如果没有对安全策略做出明确的规定，那么实际上是采用系统默认设置，即允许访问所有的资源，这样的安全策略并不能够判定什么服务可以或不可以接受，因而存在潜在的危险。在充分考虑投资和安全要求的前提下，应该采取合理的安全策略。

1.1.3 网络安全技术简介

随着网络的逐步普及，网络安全已成为 Internet 的焦点，它关系着 Internet 的进一步发展和普及，甚至关系着 Internet 的生存。可喜的是那些互联网专家们并没有令广大 Internet 用户失望，网络安全技术也不断出现，使广大网民和企业有了更多的放心，下面就网络安全中的主要技术作一简介，希望能为网民和企业在网络安全方面提供一个网络安全方案参考。

1. 杀毒软件

杀毒软件是用得最为普遍的安全技术方案，因为这种技术实现起来最为简单，但大家都知道杀毒软件的主要功能就是杀毒，功能十分有限，不能完全满足网络安全的需要。这种方式对于个人用户或小企业或许还能适用，但如果个人或企业有电子商务方面的需求，就不能完全满足。但是，随着杀毒软件技术的不断发展，现在的主流杀毒软件同时能预防木马及其他的一些黑客程序的入侵。还有的杀毒软件开发商同时提供了软件防火墙，具有了一定防火墙功能，在一定程度上能起到硬件防火墙的功效，如 KV3000、金山毒霸病毒防火墙、Norton 等。

2. 防火墙技术

“防火墙”是一种形象的说法，其实它是一种计算机硬件和软件的组合。防火墙使得互联网与内部网之间建立起一个安全网关(scurity gateway)，从而保护内部网免受非法用户的侵入，也就是一个把互联网与内部网(通常指局域网或城域网)隔开的屏障。

从实现方式上来分，防火墙又分为硬件防火墙和软件防火墙两类。硬件防火墙，它是通过硬件和软件的结合来达到隔离内、外部网络的目的的，价格较贵，但效果较好，一般小型企业和个人很难实现；软件防火墙是通过纯软件的方式来达到隔离的目的的，价格很便宜，但这类防火墙只能通过一定的规则来达到限制一些非法用户访问内部网的目的。目前，软件防火墙主要有：天网防火墙个人及企业版、Norton 的个人及企业版软件防火墙，还有许多原来是开发杀病毒软件的开发商现开发的软件防火墙，如 KV 系列、KILL 系列、金山系列等。

硬件防火墙从技术上又可分为两类，即标准防火墙和双家网关防火墙。标准防火墙系统包括一个 UNIX 工作站，该工作站的两端各接一个路由器进行缓冲。其中一个路由器的接口是外部世界，即公用网；另一个则连接内部网。标准防火墙使用专门的软件，并要求较高的管理水平，而且在信息传输上有一定的延迟。双家网关(dual home gateway)则是标准防火墙的扩充，又称堡垒主机(bation host)或应用层网关(applications layer gateway)，它是一个单个的系统，但却能同时完成标准防火墙的所有功能。其优点是能运行更复杂的应用，同时防止在互联网和内部系统之间建立的任何直接的边界，可以确保数据包不能直接从外部网络到达内部网络，反之亦然。

随着防火墙技术的发展，在双家网关的基础上又演化出了两种防火墙配置，一种是隐蔽主机网关方式，另一种是隐蔽智能网关(隐蔽子网)。隐蔽主机网关是当前一种常见的防火墙配置，顾名思义，这种配置一方面将路由器进行隐蔽，另一方面在互联网和内部网之间安装

堡垒主机。堡垒主机装在内部网上，通过路由器的配置，使该堡垒主机成为内部网与互联网进行通信的惟一通道。目前技术最为复杂而且安全级别最高的防火墙是隐蔽智能网关，它将网关隐藏在公共系统之后使其免遭直接攻击。隐蔽智能网关提供了对互联网服务进行几乎透明的访问，同时阻止了外部未授权访问对专用网络的非法访问。一般来说，这种防火墙是最不容易被破坏的。

3. 文件加密和数字签名技术

与防火墙配合使用的安全技术还有文件加密与数字签名技术，它是为提高信息系统及数据的安全性和保密性，防止秘密数据被外部窃取、侦听或破坏所采用的主要技术手段之一。随着信息技术的发展，网络安全与信息保密日益引起人们的关注。目前，各国除了从法律上、管理上加强数据的安全保护外，从技术上分别在软件和硬件两方面采取措施，推动着数据加密技术和物理防范技术的不断发展。按作用不同，文件加密和数字签名技术主要分为数据传输、数据存储、数据完整性的鉴别以及密钥管理技术四种。

(1) 数据传输加密技术

目的是对传输中的数据流加密，常用的方法有线路加密和端对端加密两种。前者侧重在线路上而不考虑信源与信宿，是对保密信息通过各线路采用不同的加密密钥提供安全保护。后者则指信息由发送者端通过专用的加密软件，采用某种加密技术对所发送文件进行加密，把明文(也即原文)加密成密文(加密后的文件，这些文件内容是一些看不懂的代码)，然后进入 TCP/IP 数据包封装穿过互联网，这些信息一旦到达目的地，将由收件人运用相应的密钥进行解密，密文恢复成为可读明文。目前最常用的加密技术有对称加密技术和非对称加密技术，对称加密技术是指同时运用一个密钥进行加密和解密，非对称加密方式就是加密和解密所用的密钥不一样，它有一对密钥，称为“公钥”和“私钥”，这两个密钥必须配对使用，也就是说，用公钥加密的文件必须用相应的私钥才能解密，反之亦然。用非对称加密方式进行加密的软件目前最流行的是 PGP。

(2) 数据存储加密技术

这种加密技术的目的是防止在存储环节上的数据失密，可分为密文存储和存取控制两种。密文存储一般是通过加密法转换、附加密码、加密模块等方法实现；如上面提到的 PGP 加密软件，它不仅可以为互联网上通信的文件进行加密和数字签名，还可以对本地硬盘文件资料进行加密，防止非法访问。这种加密方式不同于 Office 文档中的密码保护，用加密软件加密的文件在解密时其内容都会作一下代码转换，把原来普通的数据转变成一堆看不懂的代码，这样就保护了原文件不被非法阅读、修改。后者则是对用户资格、权限加以审查和限制，防止非法用户存取数据或合法用户越权存取数据，这种技术主要应用于 NT 系统和一些网络操作系统中，在系统中可以对不同工作组的用户赋予相应的权限以达到保护重要数据不会被越权访问的目的。

(3) 数据完整性鉴别技术

这种加密技术目的是对介入信息的传送、存取、处理的人的身份和相关数据内容进行验证，达到保密的要求，一般包括口令、密钥、身份、数据等项的鉴别，系统通过对比验证对象输入的特征值是否符合预先设定的参数，实现对数据的安全保护。这种鉴别技术主要应用于大型的数据库管理系统中，因为一个单位的数据通常是一个单位的命脉，所以保护好公司数据库的安全通常是一个单位网管、甚至单位的主要负责人的最重要责任。数据库系统会根据

不同用户设置不同访问权限，并对其身份及权限的完整性进行严格识别。

(4) 密钥管理技术

上面讲到了数据的加密技术通常是运用密钥对数据进行加密，这就涉及到密钥管理方面的问题，因为用加密软件进行加密时所用的密钥通常不是平常所用的密码那么仅几位，至多十几位数字或字母，一般情况这种密钥达 64bit，有的达到 128bit，一般不可能完全用脑来记住这些密钥，只能保存在一个安全的地方，这就涉及到密钥的管理技术。密钥的保存媒体通常有：磁卡、磁带、磁盘、半导体存储器等，但这些都可能有损坏或丢失的危险，所以现在的主流加密软件都采取第三方认证(第三方可以是个人，也可以是公证机关)或采用随机密钥来弥补人们记忆上的不足，还是如 PGP 加密软件，不过现在的 Windows 2000 系统以及其他的加密软件都在慢慢地往这个方向发展。

4. 加密技术在智能卡上的应用

与数据加密技术紧密相关的另一项技术是智能卡技术。所谓智能卡就是密钥的一种媒体，一般就像信用卡一样，由被授权用户所持有并由该用户赋予它一个口令或密码字。该密码与内部网络服务器上注册的密码一致。当口令与身份特征共同使用时，智能卡的保密性能还是相当有效的。这种技术比较常见，也用得较为广泛，如常用的 IC 卡、银行取款卡、智能门锁卡等等。

上面介绍了目前主流的网络安全技术，但这一切的“安全”都是相对，不能寄希望有了这种种安全措施之后就能保证万无一失，任何网络安全和数据保护的防范措施是有一定的限度的。其实在看一个内部网是否安全时不仅要考察其手段，更重要的是要看对该网络所采取的各种措施的综合性，就是说在所采取的手段中所包含的不仅是物理防范，还有人员的素质等其他因素，进行综合评估，才能得出是否安全的结论。

1.2　黑客文化

1.2.1　Hacker 与 Cracker

“黑客”(Hacker)源于英语动词 hack，意为“劈砍”，引申为做一件非常漂亮的工作。在早期麻省理工学院的校园俚语中，“黑客”则有“恶作剧”之意，尤其指那种手法巧妙、技术高明的恶作剧。而日本的《新黑客词典》中，把黑客定义为“喜欢探索软件程序奥秘，并从中增长了其个人才干的人，他们不像绝大多数使用者那样，只规规矩矩地了解别人指定了解的狭小部分知识。”全球著名的微软公司在其 1996 年出版的百科全书(光盘版)里曾对黑客下了个定义：“从 20 世纪 80 年代开始，黑客这个词作为对一些人的称谓出现在计算机软件和计算机技术里。黑客有“轻蔑”的含义，通常是指喜欢通过个人计算机和拨号上网秘密地侵入另外一些计算机或计算机网络，然后查看或破坏存储在其中的数据和程序的人”。更精确地说，黑客就是指那些通过不合法的途径进入别人的网络寻找意外满足的人。在如今的公众眼中，黑客又更多地与电脑捣蛋分子联系在一起。

由这些定义看出，黑客形象在公众心目中是不断变化的。要了解这一点，必须先了解一下黑客的发展史。

一般认为，黑客起源于 20 世纪 50 年代麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。60 年代，黑客代指独立思考、奉公守法的计算机迷，他们利用分时技术允许多