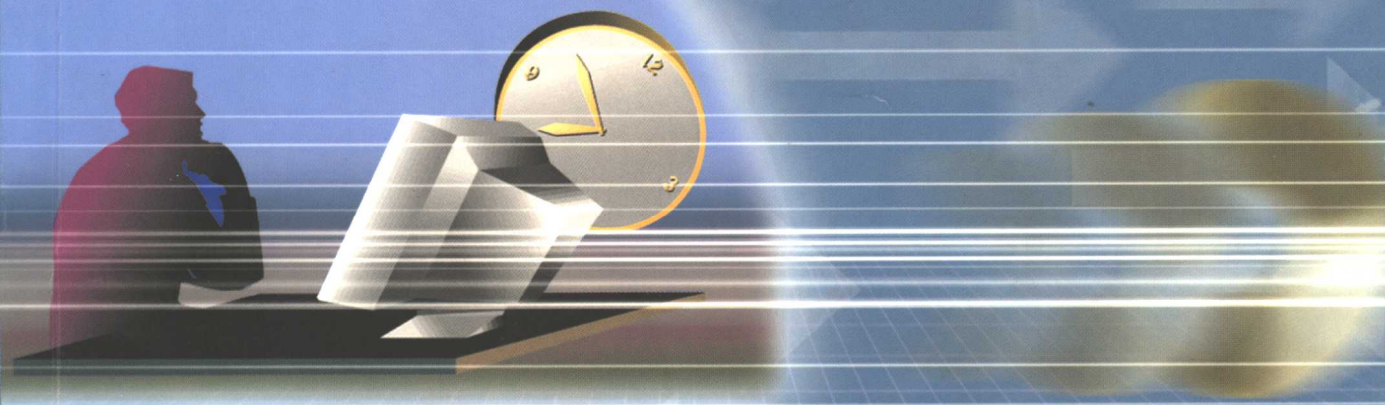
黑客攻击与安全防范

技巧及实例



李明柱　时忆杰　编著

北京航空航天大学出版社
http://www.buaapress.com.cn

黑客攻击与安全防范技巧及实例

（Windows 版）

李明柱　时忆杰　编著

北京航空航天大学出版社

http://www.buaapress.com.cn

内 容 简 介

随着网络技术的日益发展和信息技术的广泛应用，人们对信息网络的依赖程度越来越高，而非法入侵者和黑客所造成的破坏也越来越严重。本书没有阐述繁琐的信息安全理论，而是从应用的角度阐述了黑客常见的攻击手段和步骤，并提出了相应的预防措施和建议，可读性和实践性非常强。本书的内容丰富新颖，主要包括网络安全和黑客基础、Windows 安全漏洞与预防、木马攻防、口令破解、拒绝服务攻击与防范、网络炸弹攻防、活动主机探测与端口扫描、资源和用户信息扫描、通用扫描工具、病毒及其防护、OICQ 安全、浏览器安全、防火墙及应用实例、Windows 攻击与防范实例等。

本书适合于任何对网络安全和黑客入侵感兴趣的读者，特别是对网络管理员和系统管理员有重要的参考价值，也可以作为大中专院校相关专业的辅导教材。

图书在版编目(CIP)数据

黑客攻击与安全防范技巧及实例/李明柱等编著.
北京：北京航空航天大学出版社，2002.7
ISBN 7-81077-176-0

Ⅰ.黑… Ⅱ.李… Ⅲ.计算机网络 安全技术
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2002)第 028827 号

黑客攻击与安全防范技巧及实例
(Windows 版)
李明柱 时忆杰 编著
责任编辑 张光斌 范曼华
责任校对 戚 爽
北京航空航天大学出版社出版发行
北京市海淀区学院路 37 号(100083) 发行部电话：82317024 发行部传真：82328026
http://www.buaapress.com.cn
E-mail:pressell@publica.bj.cninfo.net
河北省涿州市新华印刷厂印刷 各地书店经销
*
开本：787×1 092 1/16 印张：25.5 字数：653 千字
2002 年 7 月第 1 版 2002 年 7 月第 1 次印刷 印数：5 000 册
ISBN 7-81077-176-0/TP·098 定价：45.00 元(附光盘 1 张)

前 言

早在十几年前，人们对网络的认识还很模糊，认为网络都是离我们很遥远的事情，是可有可无的东西，更不知道 Internet 和电子邮件为何物，对于电子商务更多的是概念和书本上的东西，网络购物、网络会议和网络战争等都只能在科幻小说和电影中才能体验到。但社会的发展令人吃惊，短短十几年的时间，这一切都变成了现实，并且深入到每一个人的生活之中，深刻影响着生活的每一个方面，社会也进入了一个全新的网络时代和信息时代。

随着信息网络对人们影响的不断增加，人们对网络的关注程度也越来越高，也大大增加了对信息网络的投入和建设，如扩展网络、提高系统容量和性能等，但有一点却被绝大多数人所忽视，那就是安全。安全技术在很多人的印象中都是可以不需要的东西，甚至是一种富人才需要的奢侈品，但越来越多“血”的教训不断在提醒着人们，网络安全是网络建设中的重中之重。在现今的信息时代，几乎每一个相关的人或机构都或多或少地遭受过非法入侵者的破坏和骚扰，有些还是致命性的。

网络是一个虚拟的社会，在很多方面与真实的世界有惊人的相似。在现实社会中，存在着各种各样的冲突和矛盾，如违法犯罪和战争等。犯罪分子或其他人利用各种方式和工具对个人、社会和团体等进行着不同形式的骚扰和破坏，但社会也有法律、社会规范和相应的团体与机构维护社会安全和稳定，由此产生了一对具有尖锐矛盾的对立体。随着社会的进步和发展，破坏和骚扰的形式和内容也在不断更新，相应的防范措施也在不断增强。

社会中的对立和冲突在网络中有惊人的体现，特别是由于网络的开放性，这种对立和冲突显得更为严重和紧迫。网络中存在着各种各样的黑客和非法入侵者，他们利用各种方式和工具对网络进行骚扰和攻击，轻者让受害者虚惊一场，重者泄漏和破坏用户数据，甚至使用户系统完全崩溃。同样，针对黑客的攻击和网络安全的脆弱性，人们也设计了相应的网络安全防护系统，并取得了很大的成效，许多软件和硬件提供商也在其产品中增加了黑客防护功能。

鉴于网络安全的严峻性，所以，增强普通用户的安全意识，了解和掌握必要的网络安全和黑客防护技术成为当务之急。“知己知彼，百战不殆”。要想预防和避免黑客的攻击和破坏，必须了解和掌握黑客的攻击方法和步骤，并在此基础上提供相应的安全防护措施。

本书没有介绍繁琐的网络安全理论，而是从普通用户的角度出发，详细披露了多种黑客的攻击方法和步骤，并在此基础上介绍了对应的解决措施。本书内容丰富，主要包括网络安全和黑客基础、Windows 安全漏洞与预防、木马攻防、口令破解、拒绝服务攻击防范、网络炸弹攻防、活动主机探测与端口扫描、资源和用户信息扫描、通用扫描工具、病毒及其防护、OICQ 安全、浏览器安全、防火墙及应用实例、Windows 攻击与防范实例等。通过本书的学习，可以让广大读者深入了解常见的黑客攻击方法和步骤，从而更好地进行预防，提高网络安全意识，增强网络和主机的防护能力。

本书附光盘 1 张，给出了书中介绍的所有工具的共享版或测试版以及部分软件的下载网址，希望遵守各软件对使用权限和范围的约定。

本书中介绍的技术和工具主要基于 Windows 平台，如 Windows 9x、Windows 2000 和

Windows XP。

本书是一个团队合作的成果，参与本书编写的除封面署名作者外，单　肃、王西平、李爱萍、时　间、朱雨尘、赵璐瑾、赵　琪、王　佳、吕　磊、赵先启、刘　刚、李爱红等也参加了本书的编写工作，时忆东、李以华、张光升、刘新军、王庆光、章忠伟、郭守标、李殿仁、范　凯、徐　苓、王旭超、吕　刚、李堪东、李云华等对资料整理做了大量的工作，秦爱山、马发良、巴玮晔、张　锐、郭名山、王亚楠、周　海、田宪刚、宋文献等参加了本书的测试、录排和校对等工作，在此一并表示感谢。

由于网络安全的发展日新月异，加之作者水平有限，书中错误之处在所难免，希望广大读者批评指正。

作　者

2002 年 4 月

目　录

第 4 章 Windows 安全漏洞与预防

第 5 章 大战特洛伊木马实例

第 6 章 口令破译与攻击

第 1 章　网络安全技术

随着信息技术的发展，作为信息共享和交流的手段，网络也越来越普及，人们对网络的依赖程度也越来越高，从而也为黑客的恣意入侵和破坏提供了温床，所以，如何保证网络的安全成为网络设计者和使用者所关心的话题，从而诞生了网络安全技术。

本章首先讨论一般的网络安全概念，然后对作为安全操作系统的 Windows NT、Windows 2000 和 Windows XP 的安全性进行简单阐述，接下来对常用的网络安全技术进行讨论，最后对常见的网络安全协议进行描述。

1.1　引　言

随着通信技术和网络技术的不断发展，网络在政治、军事、金融、商业、交通、电信和文教等方面的作用日益增大，而社会对计算机网络的依赖也日益增强，尤其是计算机技术和通信技术相结合所形成的信息基础设施建设，已经成为反映信息社会特征最重要的特征。随着网络的开放性、共享性和互联程度的扩大，特别是 Internet 的出现，网络的重要性和对社会的影响也越来越大。随着网络上各种新业务的兴起，如电子商务、电子现金、数字货币、网络银行等，使得网络的安全问题显得越来越重要，并发展成为影响网络发展和应用的瓶颈。

1983 年 10 月 24 日，美国著名的计算机安全专家、AT&T 贝尔实验室的计算机科学家 Rober Morris 在美国众议院科学技术会议运输、航空、材料专业委员会上作了关于计算机安全重要性的报告，从此计算机安全成了国际上研究的热点。随着网络技术的发展，网络安全已经成了新的安全研究热点。

关于网络安全，目前还没有一个确切的定义，也不可能有一个很精确的定义。主要原因是网络的发展日新月异，更新速度惊人，针对网络的攻击和威胁层出不穷，网络防护的方式也越来越多，所以，网络的安全内涵也在不断变化。

因此，网络安全在不同的环境和应用中有不同的解释：

(1) 运行系统安全：即保证信息处理和传输系统的安全，主要包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。它侧重于保证系统正常地运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏，避免由于电磁泄漏而产生信息泄露，以保护系统的合法操作和正常运行。

(2) 网络上系统信息的安全：包括用户口令鉴别，用户存取权限控制，数据存取权限，方式控制，安全审计，安全问题跟踪，计算机病毒防治和数据加密等。

(3) 网络上信息传播安全：即信息传播后果的安全，主要包括不良信息的过滤等。它侧重于防止和控制非法、有害的信息进行传播后的后果，避免公用通信网络上大量自由传输的信息失控，其本质上是维护道德、法规或国家利益。

(4) 网络上信息内容的安全：即狭义的“信息安全”。它侧重于保护信息的保密性、真实性

和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，其本质上是保护用户的利益和隐私。

显而易见，网络安全与其所保护的信息对象有关。本质是在信息的安全期内保证其在网络上流动时或者静态存放时不被非授权用户非法访问，但授权用户却可以访问。显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。

从一般意义上讲，网络安全就是如何保证网络上存储和传输的信息的安全性。

由于网络设计之初，只考虑方便性、开放性，使得网络非常脆弱，极易受到黑客的攻击或有组织的群体的入侵，也会由于系统内部人员的不规范使用和蓄意破坏，使得网络信息系统遭到损失，产生信息泄露。为了解决这个问题，国内外很多研究机构在这方面进行了研究，主要从数据加密技术、身份认证、数字签名、防火墙、安全审计、安全管理、安全内核、安全协议、智能卡、拒绝服务、网络安全性分析、网络信息安全监测和信息安全标准化等方面做了大量的工作。

黑客是影响网络安全的最主要因素之一。他们通过一些非法手段，利用自己编写的或现成的工具来查找网络系统漏洞，然后对网络系统发动攻击，对网络的正常使用造成或多或少的危害。黑客的攻击可分为两种：主动攻击和被动攻击。主动攻击是以各种方式有选择地破坏信息的有效性和完整性，或者有些主动攻击者登录进入系统，使用并占用大量网络资源，造成资源的消耗，损害合法用户的利益，如常见的拒绝服务攻击等。被动攻击是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息，这种仅窃听而不破坏网络中传输信息的入侵者被称为被动入侵者。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。

另外，有些操作系统和网络软件本身就有系统漏洞，或留有“后门”，这些都会给非法入侵者带来可乘之机，给网络的安全带来严重的后果。

1.2 操作系统安全

操作系统是网络环境的基础，也是黑客“关注”的主要对象。操作系统的安全性如何，将会直接影响到整个网络的安全性。本节将对 Windows 系列网络操作系统的安全性进行简单评述。

1.2.1 安全级别

随着计算机安全问题逐渐被人们所重视，如何评价计算机系统的安全性，即建立一套完整的、客观的评价准则成了人们关心的热点。1983 年美国国防部提出了一套《可信计算机评估标准》TCSEC(Trusted Computer System Evaluation Criteria)，又称“桔皮书”(Orange Book)。它将计算机系统的可信程度，即安全等级划分为四大类(D、C、B、A)七个小类，其中包括从最简单的系统安全特性直到最高级的计算机安全模型技术。同样，为了使《可信计算机评估标准》中的评价方法适用于网络，美国国家计算机安全中心 NCSC 在 1987 年出版了《可信网络解释》TNI(Trusted Network Interpretation)，从网络的角度解释了《可信计算机评估标准》中的观点。《可信网络解释》明确了《可信计算机评估标准》中所未涉及到的网络及网络单元的安全特性，并阐述了这些特性是如何与《可信计算机评估标准》的评估相匹配的。

1. D 级

D 级是最低的安全形式，它没有任何安全性防护措施，任何人都可以自由访问系统和系统中的数据，且完全可信。

属于这个级别的操作系统有如下几种：

- DOS；
- Windows(包括 Windows 95)；
- Apple Macintosh System 7.1。

2. C1 级

C 级有两个安全子级别：C1 和 C2。C1 级，又称选择性安全保护(Discretionary Security Protection)系统，它描述了一种典型的用在 UNIX 系统上的安全级别。这种级别的系统对硬件有某种程度的保护，但硬件受到损害的可能性仍然存在。用户拥有注册账号和口令，系统通过账号和口令来识别用户是否合法，并决定用户对程序和信息拥有什么样的访问权。

C1 级具有如下特征：

- 所有的用户都被分组。
- 对于每个用户，必须登记后才能使用系统。
- 系统必须记录每个用户的登记。
- 系统必须对可能破坏自身的操作发出警告。
- 标准 UNIX 具有 C1 级安全。

3. C2 级

除具有 C1 级的特征外，C2 级还增加了如下特征：

- 所有的对象都有且仅有一个物主。
- 对于每个试图访问对象的操作，都必须检验权限，对于不符合权限要求的访问，必须予以拒绝。
- 有且仅有物主和物主指定的用户可以更改权限。
- 管理员可以取得对象的所有权，但不能归还。
- 系统必须保证自身不能被管理员以外的用户改变。
- 系统必须有能力对所有的操作进行记录，并且只有管理员和由管理员指定的用户可以访问该记录。

目前，能够达到 C2 级的常见操作系统有：

- UNIX 系统；
- XENIX；
- Novell 3.x 或更高版本；
- Windows NT。

4. B1 级

B 级可分为三个级别：B1、B2 和 B3。B1 级，又称为标号安全保护(Labeled Security Protection)，是支持多级安全(比如秘密和绝密)的第一个级别，除了 C2 级的安全需求外，增加安全策略模型，数据标号(安全和属性)，托管访问控制。在 B1 级中，不同的组成员不能访问对方创建的对象，但管理员许可的除外；管理员不能取得对象的所有权。

Windows NT 的定制版本可以达到 B1 级。

5. B2 级

B2 级，又称为结构化安全保护(Structured Protection)，要求计算机系统中所有的对象都加标签，而且给设备(磁盘，磁带和终端)分配单个或多个安全级别。B2 级要求所有的用户都被授予一个安全等级；安全等级较低的用户不能访问高等级用户创建的对象。

银行的金融系统通常达到 B2 级。

6. B3 级

B3 级又称为安全域机制(Security Domain)，它具有安全内核和高抗渗透能力。

7. A 级

A 级，又称为可验证的安全设计(Verity Design)，是当前桔黄皮书的最高级别，包括了一个严格的设计、控制和验证过程。系统的整体安全策略一经建立便不能修改。A 级安全性要求过高，目前还没有商品化的操作系统。

1.2.2 Windows NT 安全性

Windows NT 是微软公司推出的第一款安全操作系统，随着 Windows NT 版本的不断升级，其安全性能也在不断得到增强，并达到美国国家安全局标准 C2 级。

Windows NT 采用了多种措施来加强自身的安全特性，其中包括域用户管理方式、共享和权限设置及多安全协议支持等，但 Windows NT 也存在不可避免的安全漏洞。

Windows NT 是普通用户常用的网络操作系统，至少在 Windows 2000 发布之前是这样，当然在一些重要的应用场合，如电信和银行等重要部门还都是 UNIX 的天下。

Windows NT Server 的安全性能达到了美国国家安全局 C2 级安全标准。它支持多种安全方法，并提供许多方式来控制用户的动作，同时仍允许他们访问需要的资源。例如可以在同一个目录中对不同的文件设置不同的许可权。

安全性从一开始就嵌入在 Windows NT Server 操作系统中，而不是作为一个附加的组件。这意味着即使用户在存放重要数据的计算机上工作，仍可以保证文件和其他资源的安全性，就像用户通过网络访问计算机一样。在 Windows NT Server 中，安全性甚至提供到基本的系统功能上，如设置计算机的系统时钟。

从管理方面来看，Windows NT Server 提供了综合工具帮助管理员管理和维护环境的安全性。例如，管理员可以特意控制哪些用户有访问网络资源的权利。这些资源包括文件、目录、服务器、打印机和应用软件等，对每一个资源都可以从任何一个地点集中地管理其操作权限。

用户账号也可以集中管理。管理员可以通过方便的可视化工具指定组成员、登录时间、账号期限和其他的用户账号参数等。管理员可以审计所有与安全有关的事件，如用户访问文件、目录、打印机和其他资源，以及登录尝试等。如果用户登录失败超过指定的次数，系统可以将用户账户锁定。管理员还可以强制密码使用期限，设置复杂性规则，强制用户使用不易被破译的密码等。

从用户的观点看，Windows NT Server 的安全性是完整而又实用的。简单的密码登录就可以让用户访问相应的网络资源，而用户自己并不会看见这个过程。例如，对密码进行了系统级加密，使密码本身不直接在线路上传输，这样可以防止有人通过线路窃听盗用用户密码。用户还可以定义自己所拥有的资源的访问权限。例如，如果用户需要与其他人共享文档，可以明

确指定谁有权读写那份文档，这些操作可以很容易地通过 Windows 文件管理器来设置。当然，全局资源和重点数据的管理完全是由经过授权的管理员来进行的。

下面给出 Windows NT 下所提供的一些安全功能。

1. 域用户管理

域是 Windows NT 网络安全性和集成化管理的基本单元，它是一组 NT 服务器和工作站计算机的统称，具有一组共享的数据库和共同的安全策略。域中至少有一台称为主域控制器(PDC)的计算机负责该域所有用户账号信息的管理。另外在一个域中还可以有一个或多个备份域控制器(BDC)计算机，域中的用户账号信息可由 PDC 自动更新到 BDC，BDC 只能读取用户账号信息而不能修改，而 PDC 则对用户账号数据库有完全的控制权利。当 PDC 失效或因某种原因不能正常工作时，可利用 BDC 代替 PDC 工作，维护网络的正常运转。

在由多个域组成的网络中，每个域都有自己独立的账号数据库，并有自己独立的网络运行环境，默认时不能相互通信。Windows NT 通过定义域之间的信任关系来允许在一个域中(称为该用户的本地域)定义的用户可以在另一个域中来验证身份，并可访问其网络资源。当建立了域中的信任关系以后，即信任域可以“信任”被信任域，则来自被信任域中的所有用户和用户组都可以在信任域中使用；可以在任意一台信任域的工作站上登录并访问许可的网络资源；可放在本地组中，并可在信任域中获得准许和权限。

Windows NT 中也可使用委托管理工具赋予操作员来管理域中某一特定用户账号或用户组账号的权力，并限定其委托管理范围。通过域之间的信任关系和委托管理，可以简化大型网络中的用户账号和资源管理。

2. 共享和权限设置

Windows NT 采用了 NTFS 文件系统来加强其文件的安全使用，可以根据需要设置多项安全措施，所以用于构建 Intranet 或连接 Internet 的 Windows NT 计算机最好使用 NTFS 文件系统。

在 Windows NT 中选择某一文件或文件夹，如 D:\WINNT40，右击，在弹出式菜单中选择“属性”项，弹出如图 1-1 所示的对话框。在此对话框中可以设置文件夹的普通属性、Web 共享(如果安装了 IIS，并且该服务已经启动)、共享和安全性。在图 1－1 中选择“属性”右边的复选框，可以设置该文件夹的属性，包括只读、档案、压缩、隐藏和系统等。

3. 多安全协议

为了与广大客户保持最大的兼容性，实现更严格的安全措施，以及同异构网络(如 Internet)的互联，Windows NT 可以支持多种安全协议，这也适应现今分布式计算环境的要求。Windows NT 体系结构使用通用的 Win32 安全 API，将应用程序和不同安全协议的实现细节隔离开，通过调用参数和利用身份验证的 RPC 和 DCOM 所提供的高层次接口来实现各种安全服务。

目前，Windows NT 主要支持以下几种安全协议：

(1) NTLM　NTLM 是 Windows NT LAN Manager 的缩写，它是 Windows NT 4.0 和以前版本使用的身份验证协议。NTLM 还会在以后的 Windows NT 版本中得到支持，用于同早期 Windows NT 版本进行传递式网络身份验证，远程文件访问和经身份验证的 RPC 连接。

(2) Kerveros v5.0　Kerberos 是 Windows NT 中取代 NTLM 协议来作为 Windows NT 域内或域间相互访问的主要安全身份验证协议。Kerberos 是成熟的 Internet 身份验证标准，