金桥电脑工作室

新世纪实用型信息技术人才培养教育系列

黑客攻击与防范技巧

科学技术文献出版社

★新世纪实用型信息技术人才培养教育系列（全六册）

黑客攻击与防范技巧

金桥电脑工作室 编著

科学技术文献出版社

内容介绍

本书主要介绍了 Windows 操作系统的漏洞和安全隐患，并提供了相应的防范措施。书中还介绍了黑客的基本常识和入侵技术，并教给了读者防范黑客的方法。本书的后半部分，主要针对喜欢上网的朋友，特别介绍了网络安全知识。

通过对本书的学习，可以预防绝大多数黑客的攻击和病毒带来的不必要的麻烦和损失，可以放心在网络中遨游。总之，对广大的 Windows 用户和上网的朋友来说，本书是一本不可多得的好书，拥有了它，你的电脑就拥有“安全”。

图书在版编目（CIP）数据

新世纪实用型信息技术人才培养教育系列.3.黑客攻击与防范技巧/金桥电脑工作室 编.-北京:科学技术文献出版社，2003.5

ISBN 7-5023-4195-1

Ⅰ.黑… Ⅱ.金… Ⅲ.（1）电子计算机-基本知识 Ⅳ.TP3

中国版本图书馆 CIP 数据核字（2002）第 088833 号

新世纪实用型信息技术人才培养教育系列（全六册）

——黑客攻击与防范技巧

*

金桥 夏雨 编著

责任编辑：红鸟

*

科学技术文献出版社出版

全国新华书店经销

西南师范大学教材印刷厂印刷

*

开本 787×1092 1/16 印张 19.5 字数 400 千字

版次 2003 年 5 月第 1 版 2003 年 5 月第 1 次印刷

印数：0001～5000 册

*

ISBN 7-5023-4195-1/TP· 3

全套定价：156.00 元（本册定价：26.00 元）

目 录

黑客攻击与防范技巧

目 录

第一章 Windows系统安全隐患

第一节 Windows家族产品简介

1. Windows 3. X

这是个人操作系统的一个里程碑。操作命令的图形化，使其易用易学，但是由于技术和设计上的不成熟，Win3.X当时并未在个人操作系统领域里“一统江湖”。

2. Windows 95

这是Windows家族系列的一个里程碑，虽然Win95功能不健全，频繁死机，安全隐患重重等等，但是，微软正是靠Win95才垄断了个人操作系统市场的。所以Win95应该是微软的骄傲。

3. Windows 97/98/ME/SE

这些只能说是Win95的升级版，只是在功能和安全方面做了很多弥补工作而已。

4. Windows NT/2000

这两种操作系统一般多用在网络作服务器使用：NT在局域网领域比较受欢迎，在网络中因为其安全性不佳正逐渐被Win2000所替代。Win2000因为对硬件配置要求较高，因此市场普及还需要一段时间。

5. Windows XP

虽说微软号称这是个人操作系统领域里的第二个里程碑，但是总的感觉来说XP并没有实现从win3. X到Win95那种质的飞跃。

XP的总容量居然达到1.2G，据说程序代码就有4000万行之多，并且号称“永不死机”。是不是真的不死机呢？当然，你用了就知道。不过，奉劝一句，没有P4的配置，你最好还是别“玩”它。

第二节 Windows漏洞释义

一、什么是Windows漏洞

系统漏洞也称安全缺陷，这些安全缺陷会被技术高低不等的入侵者所利用，从而达到

控制目标主机或造成一些更具破坏性的目的。

二、为什么会存在漏洞

漏洞的产生应该大致可分为两类：

1. 在程序编写过程中，编程人员为了达到不可告人的目的，有意的在程序的隐蔽处留下各种各样的后门，供日后使用，随着法律的完善，这类漏洞将越来越少（别有用心的除外）。

2. 由于编程人员的水平问题，经验和当时安全技术加密方法所限，在程序中总会或多或少的有些不足之处，这些地方有的影响程序的效率，有的会导致非授权用户的权利提升。安全与不安全从来都是相对的。

第三节　Windows内嵌的网络协议

网络中不同的工作站、服务器之间能传输数据，源于协议的存在。随着网络的发展，不同的开发商开发了不同的通信方式。为了使通信成功、可靠，网络中的所有主机都必须使用同一语言，不能带有方言。因而必须开发严格的标准，定义主机之间的每个包中每个字中的每一位。这些标准来自于多个组织的努力，约定好通用的通信方式，即协议。

现今已经开发了许多协议，但是只有少数被保留了下来。那些协议的淘汰有多种原因——设计不好、实现不好或缺乏支持。而那些保留下来的协议经历了时间的考验并成为有效的通信方法。当今局域网中最常见的三个协议是Microsoft的NetBEUI、NOVELL的IPX/SPX和交叉平台TCP/IP。

一、TCP/IP协议

每种网络协议都有自己的优点，但是只有TCP/IP允许与Internet完全的连接。TCP/IP是在60年代由麻省理工学院和一些商业组织为美国国防部开发的，即便遭到核攻击而破坏了大部分网络，TCP/IP仍然能够维持有效的通信。Arpanet就是基于协议开发的，并发展成为作为科学家和工程师交流媒体的Internet。

Internet公用化以后，人们开始发现全球网的强大功能。Internet的普遍性是TCP/IP至今仍然使用的原因。常常在没有意识到的情况下，用户就在自己的PC上安装了TCP/IP栈，从而使该网络协议在全球应用最广。

1. TCP/IP整体构架

传统的OSI(开放式系统互连)参考模型，是一种通信协议的7层抽象的参考模型，其中每一层执行某一特定任务。该模型的目的是使各种硬件在相同的层次上相互通信。这7层是:物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。而TCP/IP协议并不完全符合OSI的七层参考模型，它采用了4层结构，每一层都呼叫它的下一层所提供的网络来完成自己的需求。

这4层分别为：

●应用层：应用程序间沟通的层，如简单电子邮件传输协议(SMTP)、文件传输协议(FTP)、网络远程访问协议(Telnet)等；

●传输层：此层提供了节点间的数据传送服务，如传输控制协议(TCP)、用户数据报协议(UDP)等，TCP和UDP给数据包加入传输数据并把它传输到下一层中，这一层负责传送数据，并且确定数据已被送达并接收；

●网络层：负责提供基本的数据封包传送功能，让每一块数据包都能够到达目的主机(但不检查是否被正确接收)，如网际协议(IP)；

●网络接口层：对实际的网络媒体的管理，定义如何使用实际网络(如Ethernet、Serial Line等)来传送数据。

2. TCP/IP中协议的功能

●IP协议

网际协议IP是TCP/IP的心脏，也是网络层中最重要的协议。

IP层接收由更低层(网络接口层：例如以太网设备驱动程序)发来的数据包，并把该数据包发送到更高层——TCP或UDP层；相反，IP层也把从TCP或UDP层接收来的数据包传送到更低层。IP数据包是不可靠的，因为IP并没有做任何事情来确认数据包是按顺序发送的或者没有被破坏。IP数据包中含有发送它的主机的地址(源地址)和接收它的主机的地址(目的地址)。

高层的TCP和UDP服务在接收数据包时，通常假设包中的源地址是有效的。也可以这样说，IP地址形成了许多服务的认证基础，这些服务相信数据包是从一个有效的主机发送来的。IP确认包含一个选项，叫做IP Source Routing，可以用来指定一条源地址和目的地址之间的直接路径。对于一些TCP和UDP的服务来说，使用了该选项的IP包好像是从路径上的最后一个系统传递过来的，而不是来自于它的真实地点。这个选项是为了测试而存在的，说明了它可以被用来欺骗系统来进行平常是被禁止的连接。那么，许多依靠IP源地址做确认的服务将产生问题并且会被非法入侵。

●TCP协议

如果IP数据包中有已经封好的TCP数据包，那么IP将把它们传送到TCP层。TCP将包排序并进行错误检查，同时实现虚电路间的连接。TCP数据包中包括序号和确认，所以未按照顺序收到的包可以被排序，而损坏的包可以被重传。TCP将它的信息送到更高层的应用程序，例如Telnet的服务程序和客户程序。应用程序轮流将信息送回TCP层，TCP层便将它们向下传送到IP层、设备驱动程序和物理介质，最后到接收方。

面向连接的服务(例如Telnet、FTP、Rlogin、Xwindows和SMTP)需要高度的可靠性，所以它们使用了TCP。DNS在某些情况下使用TCP发送和接收域名数据库，但使用UDP传送有关单个主机的信息。

●UDP协议

UDP与TCP位于同一层，但不提供任何顺序或重新排序功能，因此，UDP不被应用于那些使用虚电路的面向连接的服务，UDP主要用于那些面向查询——应答的服务，例如NFS。欺骗UDP包比欺骗TCP包更容易，因为UDP没有建立初始化连接(也可以称为握手，因为在两个系统间没有虚电路)，也就是说，与UDP相关的服务面临着更大的危险。

●ICMP协议

ICMP与IP位于同一层，它被用来传送IP的控制信息。它主要是用来提供有关通向目的地址的路径信息。ICMP的“Redirect”信息通知主机通向其他系统的更准确的路径，而“Unreachable”信息则指出路径有问题。另外，如果路径错误，ICMP可以使TCP连接“体面地”终止。Ping是最常用的基于ICMP的服务。

二、NetBEUI协议

NetBEUI是为IBM开发的非路由协议，用于携带NetBIOS通信。NetBEUI缺乏路由和网络层寻址功能，既是其最大的优点，也是其最大的缺点。因为它不需要附加的网络地址和网络层头尾，所以很快并很有效且适用于只有单个网络或整个环境都桥接起来的小工作组环境。

因为不支持路由，所以NetBEUI永远不会成为企业网络的主要协议。NetBEUI帧中唯一的地址是数据链路层媒体访问控制(MAC)地址，该地址标识了网卡但没有标识网络。路由器靠网络地址将帧转发到最终目的地，而NetBEUI帧完全缺乏该信息。

网桥负责按照数据链路层地址在网络之间转发通信，但是有很多缺点。因为所有的广播通信都必须转发到每个网络中，所以网桥的扩展性不好。NetBEUI特别包括了广播通信的记数并依赖它解决命名冲突。一般而言，桥接NetBEUI网络很少超过100台主机。

近年来依赖于第二层交换器的网络变得更为普遍。完全的转换环境降低了网络的利用率，尽管广播仍然转发到网络中的每台主机。事实上，联合使用100-BASE-T Ethernet,允许转换NetBIOS网络扩展到350台主机，才能避免广播通信成为严重的问题。

三、IPX/SPX协议

IPX是NOVELL用于NetWare客户端/服务器的协议群组，避免了NetBEUI的弱点。但是，也带来了新的弱点。IPX具有完全的路由能力，可用于大型企业网。它包括32位网络地址，在单个环境中允许有许多路由网络。

IPX的可扩展性受到其高层广播通信和高开销的限制。服务广告协议(Service Advertising Protocol，SAP)将路由网络中的主机数限制为几千。尽管SAP的局限性已经被智能路由器和服务器配置所克服，但是，大规模IPX网络的管理仍是非常困难的工作。

第四节　TCP / IP 的缺陷与攻击、防御

一、TCP/IP 的缺陷

因特网的基石是 TCP/IP 协议，该协议在实现上力求效率，而没有考虑安全因素，因为那样无疑增大代码量，从而降低了 TCP/IP 的运行效率，所以说 TCP/IP 本身在设计上就是不安全的。下面是现存的 TCP/IP 协议的一些安全缺陷：

1.很容易被窃听和欺骗

大多数因特网上的流量是没有加密的，电子邮件口令、文件传输很容易被监听和劫持，