一个洗心革面的黑客指导你如何
保护Windows 2000服务器和网络

Maximum Windows 2000 Security

Windows安全

黑客谈

[美] Anonymous 著
詹文军 等译

电子工业出版社

Windows安全黑客谈

Maximum Windows 2000 Security

[美] Anonymous 著

詹文军 等译

電子工業出版社
Publishing House of Electronics Industry
北京 · Beijing

内 容 简 介

本书主要介绍了 Windows 2000 网络环境中各个方面的安全性。书中指出了为什么学习攻击 Windows 2000 是一种良好的防御措施。全书对黑客攻击和安全性工具进行了介绍，揭示了特洛伊木马和后门程序的内部工作机制，使读者了解活动目录的长处和弱点。并且讲解了如何保护 Web 和因特网服务，揭示了拒绝服务攻击和欺骗攻击的工作原理，介绍了 TCP/IP 过滤和有效的防火墙及实现 Windows 2000 私密性、加密以及 VPN 和 IPSec 的方法。此外，还讲述了如何使用有效的记录、入侵检测和备份功能来维护 Windows 2000 系统的安全性，概括了 Windows 2000 的网络安全性体系结构。

本书适用于那些需要保护他们的 Windows 2000 服务器和工作站以防范非法入侵以及其他破坏系统完整性的外部威胁的系统管理员和 Windows 2000 用户。

版权贸易合同登记号　图字：01-2000-3553

图书在版编目（CIP）数据

Windows 安全黑客谈 /（美）Anonymous（匿名）著；詹文军等译. - 北京：电子工业出版社，2002.7
书名原文：Maximum Windows 2000 Security
ISBN 7-5053-7861-9

Ⅰ. W…　Ⅱ. ①匿… ②詹…　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 054943 号

责任编辑：李秦华　陶淑毅
印 刷 者：北京天竺颖华印刷厂
出版发行：电子工业出版社　www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编：100036
经　　销：各地新华书店
开　　本：787 × 1092　1/16　　印张：27　字数：674 千字
版　　次：2002 年 7 月第 1 版　　2002 年 7 月第 1 次印刷
定　　价：43.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077

目　录

第一部分　Windows 2000 Server 安全性介绍

第二部分　Windows 2000 Server 安全性基础

第三部分 Windows 2000 联网

第一部分
Windows 2000 Server 安全性介绍

第1章　攻击Windows 2000服务器

本章要点：

- 什么使得Windows 2000易于遭受攻击
- 了解工具

从传统意义上来说，黑客（hacker）是指那些具有超常编程水平或计算机系统知识的人，这些人能够以设计者始料未及的方式对某个系统或编程语言进行操纵。曾几何时，被人称为黑客是一件无上光荣的事情，因为这意味着对计算机系统具有超乎常人的知识水准。

然而，当现如今人们听到“黑客”一词时，大多数人便会联想到那些以恶意方式侵入计算机系统的人。遗憾的是，由于媒体对黑客一词的误用使得该词几乎失去了其原本的含义。相信许多人更愿意使用“计算机窃贼（cracker）”或“攻击者（attacker）”来指代那些不法之徒，但在本书中，我们将以公共流行的方式来使用黑客这一名词——那些使用自己的知识绕过系统的安全性措施来访问网络资源的人。本书对黑客的定义既包括了具有恶意的人，也包括了那些具有善意的人，因为不管其意图如何，他们终究是擅自闯入了系统。

说明： 具有恶意的黑客通常称为黑帽黑客（black hat hacker），那些闯入系统只是为了进一步提高安全性研究水平的黑客则称为白帽黑客（white hat hacker），而那些时好时坏的黑客则称为灰帽黑客（gray hat hacker）。

侵入一个Windows 2000服务器的人可以具有许多动机，其中一些是为了个人目的，其他一些则是为了进行安全性审核才这样做，而还有一些人则是为追求这种挑战所带来的刺激。但不管黑客的动机是好是坏，要了解另一方——系统管理员的作为是很重要的，如果黑客的动机具有恶意，则他应当了解系统管理员采取了什么措施来保护Windows 2000服务器；如果黑客的动机没有恶意，则了解对方的行为同样很重要。本章的内容不管对于黑客还是系统管理员而言，应当都会有帮助。

在人们发现我（本书的首席作者以前曾是个黑客——译者注）具有几乎各方面的黑客技能之后，没过多长时间他们就请求我将自己所了解的东西都传授给他们，我尽量向他们推荐Internet上的教程，但是大多数人希望能够得到快速入门诀窍，使得他们能够在30分钟左右就能够成为一个黑客，不过事实上成为一个黑客却没有捷径，这需要长期不懈的学习和足够的耐心。

因此，在打消人们迅速成为黑客的梦想之后，那些人接着问我应当从何开始做起？这个问题的答案很简单——从任何地方开始都可以，换句话说，你可以从任何一个可供利用的Windows漏洞开始，并从各种角度来学习利用该漏洞的知识；然后，你可以再接着学习下一个，并了解该漏洞的各方面知识，最终你将得到一个完整的黑客知识库，随时可以在需要时从中提取必要的知识。

为了解如何攻击Windows 2000，你应当：

- 了解该操作系统
- 了解其弱点
- 了解黑客工具

到目前为止，大多数想做黑客去攻击系统的人都已经放弃该念头了，只有那些真正感兴趣的人才会继续并花费大量时间去学习各种黑客技能，这正是一个真正的黑客和“脚本鼠”（script kiddie）之间的区别，脚本鼠是那些使用在 Internet 上所找到的现成工具或脚本的人，他们甚至不了解自己在做什么，或者在没有工具可用时便不知所措了。

遗憾的是，由于 Internet 上充斥着许多黑客工具，脚本鼠也随之泛滥，另外，在网络上仍然具有许多带有旧的安全性漏洞的服务器，脚本鼠使用工具就可以成功地攻击这些服务器，但是对于有经验的系统管理员来说，脚本鼠并不是很大的威胁，对于系统管理员而言，脚本鼠通常很容易露出马脚而被察觉到。

一个更有经验的黑客对他所攻击的操作系统是很了解的，他知道操作系统的长处和弱点，并且了解如何利用这些弱点，另外他还知道使用哪些工具以及如何使用这些工具来攻击系统。

1.1　什么使得 Windows 2000 易于遭受攻击

Windows 在安全性方面的声誉一向都不好，许多网络管理员仅仅因为这一点而不愿意使用它，但事实是任何操作系统如果配置不正确都可能具有安全性方面的弱点，Windows 2000 自身并没有先天性的安全性弱点，只要恰当地配置它，Windows 2000 可以非常安全。另外，每个操作系统都具有长处和弱点，以下是使 Windows 2000 易于遭受攻击的主要因素：

- 用户（包括系统管理员）
- 寻求 Windows 的开放性
- 难以进行有效的监视
- Windows 2000 自身的规模和复杂性
- 脆弱的盒外（Out-of-the-box）安装性

1.1.1　用户脆弱性

用户是操作系统中最主要的脆弱点，但是由于 Windows 2000 很容易使用，使得它具有一个庞大的初学者群。而对于系统管理而言也同样如此，Windows 2000 使得学习成为一个网络管理员如此之容易，以至于那些在诸如网络协议和网络安全性等领域知之甚少的人也能够成为网络管理员。

更糟糕的是，许多小型的公司由于不能支付一个全职网络管理员的薪水，因此，它们常常将网络管理任务交给某个看起来对 Windows 操作系统最了解的用户来完成，这样所导致的结果是，常常是只有三脚猫水平的网络管理员为用户分配了安全性较弱的密码，那些易于遭受攻击的服务仍然在操作系统中运行，最新发布的补丁程序未能及时安装，情况之糟可想而知。

当你对常见的用户脆弱性有所了解后，将会知道如何利用这些弱点来发动攻击。

1.1.2 Windows的开放性

Windows是一个为微软公司带来可观收入的产品，为了使该产品能够一直盈利，微软公司必须保持它在操作系统市场上的主宰地位，这意味着Windows必须比和它竞争的操作系统具有更多的优势，并且这一点通常意味着微软公司必须一直不断地在Windows中加入新的功能，这些功能通常着眼于诸如互操作性、集成性和可扩展性等领域，当这些功能被加入时，Windows便在应用程序开发、网络连接和通信等方面具有了更进一步的开放性。开放性所带来的问题是，每个新的服务都引发了一系列全新的必须处理的安全性问题，而且通常以开放性思想进行代码编写的程序员不会想到其中所涉及的安全性风险。因为开放性的思想倾向和安全性思想倾向是矛盾的。

例如，为了扩展微软的COM技术的适用范围，微软创建了一种称为远程数据服务（RDS，Remote Data Service）的服务，这种服务允许用户完成许多事情，诸如远程数据访问，但是这种开放性引发了一个非常大的安全性漏洞，使得Internet上的任何人都可以在某个Windows NT服务器上运行自己所希望的命令。当然，RDS的开发者并不会想到他们所开发的数据服务会被用来对如此之多的Windows服务器进行攻击。

如果用户查看一下在默认的Windows 2000安装过程中所安装的服务，将不禁会想知道在将来究竟会在其中发现多少安全性漏洞，其中一些令我们感到不安的服务如下：

- Internet连接共享（Internet Connection Sharing）
- NetMeeting远程桌面共享（NetMeeting Remote Desktop Sharing）
- 远程访问自动连接管理器（Remote Access Auto Connection Manager）
- 远程注册表服务（Remote Registry Service）
- 终端服务（Terminal Service）
- 站点间消息（Intersite Messaging）

1.1.3 难以进行有效的监视

另外一个折磨Windows 2000的问题是它缺乏有效的监视工具。Windows 2000的确具有事件日志（Event Log）程序，但是根据作者本人的经验，很少有系统管理员会真正定期地查看他们的事件日志。

问题在于一般的系统管理员将打开事件查看程序（Event Viewer），并且从中看到的是一大堆和安全性有关的事件，一些是对成功进行了审核，另一些则是对失败进行了审核，这些事件是用无意义的代码，例如529，681和577。大量含义不明了的事件使得管理员很难从Event Viewer中察觉到系统被入侵，即使是用户觉察到这一点，Event Viewer也通常不会记录相关的信息，例如进行入侵的远程IP地址等。

我曾经在Windows 2000计算机上运行过多次渗透性测试（Penetration test），并且这些计算机的系统管理员从未察觉到我的举动。我经常向系统管理员询问他们是否察觉到自己的计算机被攻击过，如果是，他们又是如何发现的。在大多数情况下，他们承认自己不知道曾经被攻击过。当我问到他们最后一次查看事件日志的时间时，答案通常是在几个月之前，甚至是更久以前。

在Windows 2000中，如果没有第三方软件的帮助，通常是很难或者是不清楚如何回答诸如

以下的问题：

- 此时是谁连接到我的计算机上？
- 某人最后一次使用终端服务进行登录是什么时候？
- 针对某个账号所尝试的密码猜测失败次数是多少？
- 目前是否有其他人使用我的账号从其他计算机上登录？
- 目前是否有其他人有映射到我的计算机上的共享？

很明显，如果没有好的监视方式，是很难知道自己是否处于被攻击状态的，而且尽管有第三方的工具可用来对Windows 2000的各方面进行监视，但却没有一个单一的工具能够弥补Windows 2000 的缺点。用户必须使用各种工具来获得完整的监视情况。

只要Windows 2000难以被监视这种情况存在，黑客就可能会觉得他的入侵行为将不会被察觉到。而且黑客们的这种感觉有时的确如此。适当的系统监控其实是能够做到的，但是这要花费额外的工夫，而这点工夫是大多数系统管理员所不愿花费的。

说明：在第 22 章中可以了解更多有关 Windows 事件日志的内容。

1.1.4　Windows 2000 自身的规模和复杂性

就在不长的时间以前，操作系统在一个单面的 360 KB 的软盘上就可以全部存储下，而如今却相反，Windows 2000 是一个庞大的操作系统，具有上千万行的代码，同时这些代码中的大部分都是在 1 年到 2 年之前所编写的（即大部分代码都是新编写的），由于具有如此之多的代码而且是新代码，使得许多可能损害系统安全性的漏洞得以藏身，更何况在网络上还有大量的黑客在一直对 Windows 2000 虎视眈眈以发现这些漏洞。

对于安全性而言，系统的复杂性从来就不是一件好事。黑客可以很容易地利用 Windows 2000的复杂性来进行攻击，例如，如果某个黑客打算将一个特洛伊木马程序放置到某个WINNT 目录下，同时将该程序命名得更冠冕堂皇一些，例如称为tapi.exe，则该程序将会很容易地和目录下的其他系统可执行文件混杂在一起而不被人察觉。类似地，如果这样一个程序在任务管理器（Task Manager）中显示为正在运行，则可能不会引起管理员的警惕，原因在于许多管理员不会注意运行的大部分应用程序的名称。这非常类似于这样一种情况：如果用户手里拿着一个公文包并煞有介事地匆匆而行，则可能会通过任何自己希望进入并且设有警卫保护的建筑物。一个看起来合法的可执行程序通常总是会被管理员盲目地作为合法程序而给予“放行”。随着 Windows 2000 的不断发展和修改，对于一个黑客来说，利用 Windows 2000 的复杂性来隐蔽自己私下进行的勾当一点也不难。

1.1.5　脆弱的盒外安装性

虽然 Windows 2000 比 Windows NT 4 更为安全，但是这两者在第一次安装时都具有相同的默认设置。安装 Windows 2000 是一个需要两步来完成的过程。首先用户需要安装操作系统，然后需要对系统进行仔细检查并加固（harden）它，加固（hardening）是关闭不必要的服务并修改系统设置使得它更不易于遭受攻击的过程。问题在于许多系统管理员忽视执行这一加固程序，

使得系统暴露于各种攻击所及的范围之内。由于这一原因，系统可能有诸如WWW发布服务等服务正在运行，而且用户可能甚至都未意识到这一点，如果用户没有意识到WWW服务正在运行，他当然就不会去监视Web日志以察觉系统是否被攻击，这一点对于许多其他的Windows 2000服务也是如此。

第一个Windows 2000的补丁程序（hotfix，MS00-006）发布于2000年1月26日，正好是在Windows 2000上市之前一个月。该补丁程序修补了Windows 2000中的一个漏洞，该漏洞使得用户可以通过使用任何Web浏览器来查看位于某个Web服务器上的敏感文件。虽然这一漏洞在编写本书时的一年前已经被修复，但目前Internet上仍有上千台Web服务器（包括那些属于许多大公司的服务器）面临遭受这一漏洞被攻击的危险。由于很容易忽略加固过程，因此许多系统在安装时都没有经历过第二步骤的加固阶段。使用合适的工具，用不了多长时间就可以确定这些系统没有安装补丁程序而保持为更新状态，如果用户扫描某个Windows 2000系统并且发现某个一年前就存在的安全性漏洞，则十有八九是在系统安装后就没有打过补丁。

说明： *在第5章中可以了解更多有关安装Windows 2000的内容。*

1.2 了解工具

“工欲善其事，必先利其器”，用户如果具有一组好用的工具，则效果会好得多。目前有许多黑客工具可用，但是寻找合适的工具却不是一件容易的事。任何一个好的黑客都具有一个自己长年累月所收集或创建的黑客工具箱。因此要成为一个好的黑客，了解什么工具可用以及如何使用是基本的要求。

黑客工具可以是Windows应用程序或控制台应用程序，它们还可以是脚本或只是批处理文件。另外，黑客工具甚至还可以包括Web站点，这些Web站点提供了有助于黑客攻击的可用联机应用程序。不管黑客工具是什么样的形式，只要用户了解了Windows 2000的弱点，就应当着眼于收集（或创建）合适的工具来利用这些弱点发起攻击。在第3章中，我们将讨论各种用户在一开始可以加入自己工具箱中的特定黑客工具。

收集黑客工具的一个重要方面是了解这些工具以及何时使用它们。许多脚本鼠所用的工具通常会很容易地在网络或系统日志中留下踪迹。了解哪些工具会容易被人察觉到，哪些工具在使用时不容易被人发现，这是工具收集过程中的一个重要组成部分。

尽管第三方创建了许多专门用于黑客攻击的工具，Windows 2000还是提供了许多内置的工具，这些工具同样值得用户考虑使用。其中一些工具包括以下内容：

- net.exe　可以用于发现计算机和网络信息，并建立网络连接
- Nbtstat.exe　可以用于显示某个远程计算机系统的NetBIOS名称表
- Tftp.exe　可以用于从黑客计算机来回传输文件
- telnet.exe　可以用于访问黑客计算机所连接的网络

用户应当花点时间去深究Windows 2000以确定是否还有其他可用的工具。此外，Windows 2000资源工具箱（Resource Kit）包含了许多在攻击Windows 2000时有用的工具。学习如何利用Windows 2000内置工具的好处是：它们已经位于用户打算要攻击的计算机系统（即Windows

2000 系统）上，这样可以不需要再增加将黑客工具转移到某个要攻击的远程计算机上的步骤，而这一步骤通常在黑客攻击过程中是很困难的一步。

黑客工具对于攻击而言是如此之重要，以至于我们可以通常凭某个黑客的工具箱来评判其技能的高低。

说明：参见第 3 章可以了解更多有关黑客工具的知识。

1.3 小结

攻击 Windows 2000 的技能是无论如何不可能在一个晚上就能够掌握的，通过学习 Windows 2000 操作系统，了解其安全性弱点并寻找合适的工具来利用这些弱点发动攻击，用户将逐步对 Windows 2000 有一个深入的了解。在熟练之后，用户将几乎能够多次渗透进入任何系统，并且在几分钟之内完成这些任务。另外，如果用户的终极目标是为了通过学习如何攻破 Windows 2000 来保护它，则你将比那些从来未真正攻破 Windows 2000 的人要老练内行得多，从而挫败他们的企图。

无论用户的目标是攻破 Windows 2000 还是保护 Windows 2000，用户都必须获得足够的技能，而这只能借助坚持不懈的学习，通过实际使用各种技术和工具来获得。

第2章　Windows 2000服务器的安全性特点

本章要点：

- Windows 2000的安全性特点
- 增强的访问控制
- 增强的网络控制
- IPSec和VPN
- Kerberos
- 高级认证支持
- 文件系统加密
- 记录

2.1　Windows 2000的安全性特点

Windows 2000和Windows NT的最初版本相比，在安全性特点方面已经历了一段很长的发展道路，在过去的几年，安全性协议已经成熟，而且Windows操作系统也历经了许多考验。在本章中，我们将讨论在Windows 2000中可用的许多安全性特点以及它们如何在提高系统整体安全性方面起作用。

2.2　增强的访问控制

除非读者是初次接触计算机的新手，否则都应当遭遇过某种形式的违背安全性的行为，即使用户可能从未意识到这一点。实际上，就在不久以前，大多数桌面操作系统都是不提供或提供很少的安全性，用户一时兴起便可以访问到其他用户的文件。

大约上个世纪最后10年左右，随着网络的流行，这种局面发生了改变，公众的安全性意识得到了增强——这种意识由计算机黑客的猖獗所催生——使得大多数用户都产生了一种有益的怀疑心理，这种情况又转而促使软件开发商逐渐在其产品中加入安全性功能以满足公众的需要。

Internet在公共安全性意识不断提高的演变过程扮演了一个重要的角色，到目前，大多数网络操作系统都提供了一种称为访问控制的安全性功能。广义上讲，访问控制是任何能够有选择地允许或拒绝用户对系统资源进行访问的技术和机制，这些系统资源包括文件、文件夹、目录、卷、驱动程序、服务、主机、网络等。

Windows 2000将所有的管理权限集中到一个单一的账号——该账号称为Administrator（管理员）账号。Windows 2000中的Administrator账号等同于UNIX中的root账号或NetWare的Supervisor账号。作为拥有Administrator账号的管理员，可以控制以下内容：