“十五”国家重点电子出版物规划项目·计算机网络技术和网络教室系列

本书列举**51**个问题，完整详实的告诉你各式各样的服务器黑客任务秘技
本书CD包含StartupCPL，TaskInfo，NetWatcher，NetScan Pro等多项黑客必备软件。

北京希望电子出版社　总策划
程秉辉 John Hawke　编　著

黑客任务实战

服务器攻防篇

- 全球最完整详尽的IIS服务器攻防实录
- 更换网页与入侵网站服务器操作流程与技巧运用
- Unicode、IIS 错误解码、CGI 解译错误等漏洞攻防操作
- .ida/idq、.printer、FP 2K ES远程溢出漏洞入侵攻防详解
- 使用 FrontPage 就可以更换别人的网页?!
- ASP 网页闻之色变的.asp远程溢出漏洞
- 让 Windows 电脑与服务器立刻死机的 SMB 漏洞攻防操作
- 清除目标服务器中的IIS与系统日志的详细操作
- 拒绝服务攻击(DoS)的完整讨论、操作与研究
- 各种漏洞与其他黑客任务的搭配使用、漏洞完全修补
- 附全球IP地址详细列表、端口列表说明

本书中所有内容都经过多次的实战测试，决不告诉你无法做到的方法！

Win9X.WinMe 完全适用 Win2k.WinXP

电脑一以用为本！
计算机应用文摘

“很强的可操作性，结构上标新立异，相当的人性化。”

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

“十五”国家重点电子出版物规划项目·计算机网络技术和网络教室系列

本书列举**51**个问题，完整详实的告诉你各式各样的服务器黑客任务秘技
本书CD包含StartupCPL，TaskInfo，NetWatcher，NetScan Pro等多项黑客必备软件。

北京希望电子出版社　总策划
程秉辉 John Hawke　编　著

黑客任务实战

服务器攻防篇

- 全球最完整详尽的IIS服务器攻防实录
- 更换网页与入侵网站服务器操作流程与技巧运用
- Unicode、IIS 错误解码、CGI 解译错误等漏洞攻防操作
- .ida/idq、.printer、FP 2K ES远程溢出漏洞入侵攻防详解
- 使用 FrontPage 就可以更换别人的网页?!
- ASP 网页闻之色变的.asp远程溢出漏洞
- 让 Windows 电脑与服务器立刻死机的 SMB 漏洞攻防操作
- 清除目标服务器中的IIS与系统日志的详细操作
- 拒绝服务攻击(DoS)的完整讨论、操作与研究
- 各种漏洞与其他黑客任务的搭配使用、漏洞完全修补
- 附全球IP地址详细列表、端口列表说明

本书中所有内容都经过多次的实战测试，决不告诉你无法做到的方法！

电脑一以用为本!
计算机应用文摘

“很强的可操作性，结构上标新立异，相当的人性化。”

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内 容 简 介

网站服务器的黑客攻防一直是网络安全中最重要的一部分。本书作者在经过数月的努力之后，终于将网站服务器的黑客攻防以深入浅出、简单易懂的方式呈现在您的眼前，让您不必具有高深的网络知识和经验，只要依照本书的操作说明来按图索骥的进行，就可以完成许多看似不能的黑客任务，让您充分了解与感受到黑客高手的技巧和行为，如此网管人员才可对症下药，防止黑客的入侵与破坏。

本书中详细的讨论了 Unicode、IIS 错误解码、CGI 解译错误等漏洞的详细攻防操作，同时针对最近几年黑客最流行的远程缓冲区溢出漏洞入侵 (Remote Buffer Overflow) 进行完整研究，包含.ida/idq、.printer、FrontPage 2K Extension Server 等漏洞的攻略操作；另外如更换网页、服务器瘫痪攻击与死机、清理服务器中的日志让黑客全身而退等内容在本书中都有详尽的讨论，再加上本书作者精心设计的漏洞扫描程序、远程溢出入侵程序和 IIS 瘫痪工具，更让黑客任务平易近人，而同时，网络管理员也将从本书中找到如何防护自己的网站的绝佳思路。

本书适合于所有上网用户增强网络安全意识，同时对网络管理员和致力于网络安全的开发人员有很大参考价值。

本书 CD 包含端口列表、各地 IP 地址详细列表、NetBrute Scanner、Clearlogs、N-Stealth 等多项黑客必备软件。

盘书系列名：“十五”国家重点电子出版物规划项目　计算机网络技术与网络教室系列
盘　书　名：黑客任务实战——服务器攻防篇
总　策　划：北京希望电子出版社
文本著作者：程秉辉 John Hawke 编写
CD 制作者：希望多媒体开发中心
CD 测试者：希望多媒体测试部
责任编辑：梅琪 大成
出版、发行者：北京希望电子出版社
地　　址：北京市海淀区知春路甲 63 号卫星大厦三层 100080
网　　址　www.bhp.com.cn
E-mail: lwm@bhp.com.cn
电话:010-62520290, 62521724, 62528991, 62630301, 62524940, 62521921, 82610344（发行） 010-62613322-215（门市）010-82675588-501,82675588-201（编辑部）
经　　销：各地新华书店、软件连锁店

排　　版：希望图书输出中心
CD 生产者：北京中新联光盘有限责任公司
文本印刷者：北京媛明印刷厂
开本 / 规格：787 毫米×1092 毫米　16 开本　30.5 印张　552 千字
版次 / 印次：2003 年 2 月第 1 版　2003 年 2 月第 1 次印刷
印　　数：0001-5000 册
本 版 号：ISBN 7-89498-081-1
定　　价：45.00 元（本版 CD）

作者感言

经过三个多月不眠不休的工作，终于将本书完成，真是千呼万唤始出来，由于之前黑客任务实战系列书中都没有详细讨论有关网站服务器的攻防，许多读者都觉得缺了一个最重要的主菜，其实小弟心里也很清楚，并非不想写这本书，而是实在不好写，其中最主要的原因是网站服务器攻防的重点在于**漏洞**，漏洞的利用是初级黑客进入中、高级黑客的必经过程，然而面对各种不同系统、不同版本、Web Server…各式各样的漏洞，哪些才是真正有利用价值，而哪些只是看看就算了，若您没有丰富的经验则实在是很难做出明确的判断，不过即使有利用价值没有适当的工具也是白搭(除非您自己会编程)，所以要如何让各位读者容易了解、很方便的利用各种漏洞就成为本书最大的挑战，为此小弟在荒废了七、八年之后，重新下海编程，终于将差强人意的成果放在本书中与各位分享…差点没劳死!!

然而美中不足的是其中还有几个很有价值的漏洞，由于小弟研究了许久一直没有将关键的地方完成，像这种研发工作(R&D)又不知道何时才会有结果，若运气好或许一两天就解决，运气不好则可能三个月或半年也没结果(这就是R&D工作的痛苦之处)，所以最后只好忍痛放弃这几个漏洞，没在本书中讨论，不过只要有成果我们一定尽快在相关书籍中发表出来。

由于现在每天要处理的信件很多，所以目前**我们只回复与书中内容或所介绍的软件有关的信件**，其他不相关的信件将不处理，请您能理解

作者感言与见谅，毕竟小弟不是Bill老大，可以依照不同的问题收取不同的费用来捞钱。另外我们并不会帮任何人或组织去破解或入侵某个网站、某台计算机或各种密码，也无法查看您的文件是否中毒、帮您测试软件、帮您找软件…等，我们很愿意帮各位解决问题，但实在无法处理这些超出范围的要求，非常谢谢您的合作!

请注意：

- 若你使用电子邮件则填写本书**光盘中的读者服务卡**。
- 下一页读者服务卡中的**电子邮件地址请写清楚**，不要太草!

请电邮到:**hawkes@ms29.hinet.net**

请注意：本书内容完全从理论与技术实务的角度来进行有关黑客攻略的讨论与研究，所以若有将本书内容使用于任何违反法律之行为，必须自行承担各种相关的法律责任，请各位读者慎之！慎之！

程秉辉

Hawke Cheng

1.7.2003

请将下表数据填妥后 EMail 到 **hawkes@ms29.hinet.net**，
我们将会不定期的提供您有关各种 Windows、Internet
与多媒体的最新信息与相关软件，请多多利用，谢谢！
您也可以到我们的网站: **http://faqdiy.diy.163.com**
来获得相关的更新文件与最新信息!!

若您使用电子邮件则请使用本书光盘中所附的读者服务卡，不必使用这个读者服务卡。

讀者服務卡 REGISTER CARD

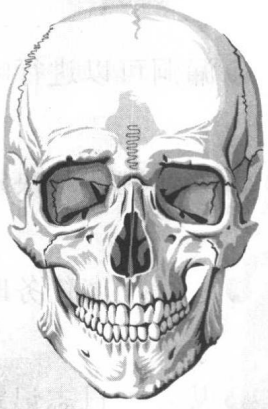
书名	**黑客任务实战-服务器攻防篇**	本书序列号	**北京希望2K30101**
姓名		性别	☐先生 ☐ 小姐
年龄			
学历	☐ 研究所 ☐ 大学 ☐ 专校 ☐ 高中职 ☐ 中学 ☐ 小学		
您的电邮地址			
传真号码			
购买地区(选择最近城市)	☐ 北京 ☐ 上海 ☐ 南京 ☐ 广州 ☐ 深圳 ☐ 武汉 ☐ 重庆 ☐ 成都 ☐ 福州 ☐ 天津 ☐ 大连 ☐ 南昌 ☐ 苏州 ☐ 杭州 ☐ 青岛 ☐ 长沙 ☐ 开封 ☐ 合肥 ☐ 哈尔滨 其它:		
职业	☐学生 ☐电脑业或 IT 部门 ☐非电脑业 ☐其他:_____	您觉得本书	☐简单 ☐适中 ☐艰深
在 Windows 中常遇到什么样的困扰与麻烦?			
您从何处知道本书	☐连锁书店 ☐ 一般书店 ☐电脑专卖店 ☐同学 ☐展览 ☐亲友 ☐广告函 ☐因特网 ☐报纸: _____ ☐杂志: _____ ☐其他: _____		
您还希望获得哪方面解决问题的信息			
您对本书有何建议			

目　录

第 1 章

服务器的攻防观念与准备工作

Basic Concept and Preparing for Hacking Web Server



相较于入侵或攻击一般上网的个人机，对 Internet 服务器进行各种黑客任务有更高的困难度与更多的挫折，因此在进行之前，本章将先帮你创建相关的基本观念与知识，内容包含：

- 有哪些方法可对 Internet 服务器进行黑客任务?
- 利用漏洞入侵或攻击 Internet 服务器的标准流程。
- 漏洞可以进行哪些黑客任务?
- 如何判断与决定对服务器进行黑客任务时需要隐藏 IP?
- 进行黑客任务时所留在服务器中的各种记录要如何清理?
- 从各种日志记录中查看找出可能的黑客入侵。
- 哪些方法可以尽可能防止各种日志文件被黑客更改或删除?

Q1 **入侵或攻击网站或服务器 (如：Web Server、FTP Server) 的原理与观念是什么?**

Q2 **对 Internet 上的各类服务器进行黑客任务有哪些方法可使用? 各有何优缺点?**

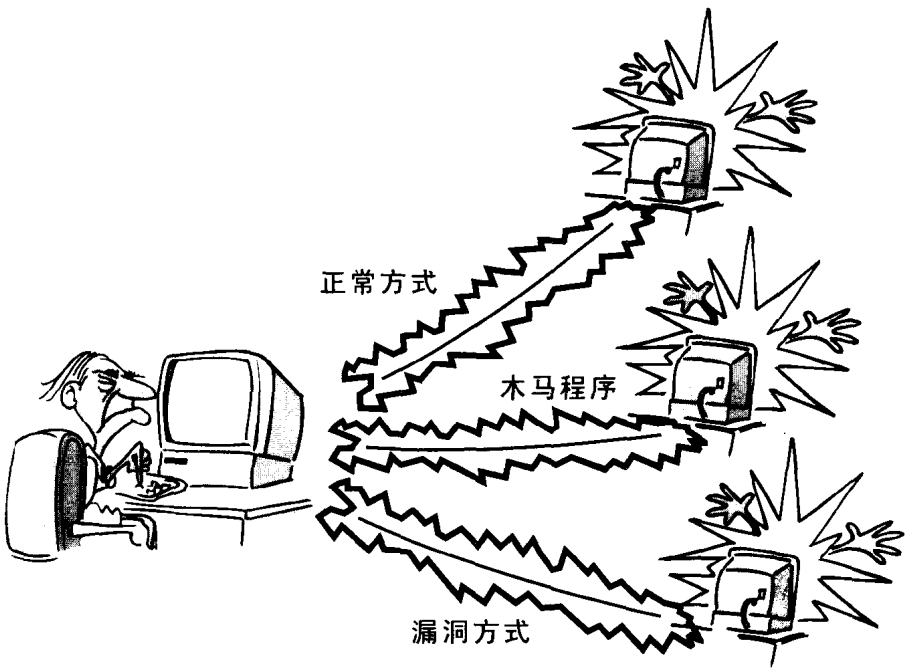
相关问题请见 Q3

在**黑客任务实战一个人机漏洞篇**中我们一再强调：绝对没有什么方法或一定可以 100% 入侵某个上网的个人机。既然一般上网的个人机都如此了，更何况具有更多安全防护 Internet 上的各种服务器 (如：Web Server、FTP Server…等)，因此这里我们也要帮各位 (特别是黑客初学者) 创建一个正确的观念…**没有什么方法可以 100% 成功的入侵或攻击某个 Internet 服务器**，成功完全决定于你不屈不挠的精神、经验的累积与运气好坏，这样了解吗?!

在本问题中我们将以 **Top-to-Down** 的方式，详细告诉你要对 Internet 上的各类服务器进行黑客任务有哪些方法? 它们有哪些优缺点? 什么情况下适用哪些方法? 然后再将各方法分散到其他问题中个别讨论，帮助你更清楚的认识与了解，所以请仔细观看。

❑ 黑客任务的方法

一般通过 Internet 来进行各项黑客任务，不外乎**正常方式、木马程序或漏洞方式**…三种方法，如下图。



下面我们就对这三种方法来分别讨论与研究。

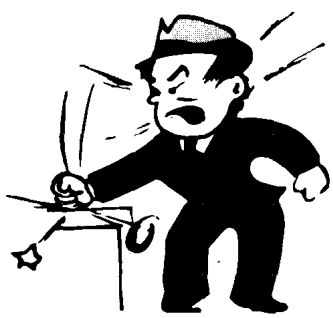
❑ 方法❶ 正常方式

所谓的正常方式就是通过 Internet 连接的方式来进入 Internet 上的各类服务器中，就像是连接到局域网 (LAN) 中的服务器一般，只是 Internet 世界是广域网 (WAN) 而不是局域网 (LAN)，而在 Windows 系统中最典型的作法就是通过端口 **139** (也就是磁盘共享) 的方式，使用**资源管理器**或**网上邻居**就可以连接进入其他服务器中，然后进行各项黑客任务，下面就来看看这个方法有哪些优缺点。

Note

此方法当然是只能进入运行 Windows 系统的服务器，若是使用 UNIX、Linux 系统的服务器当然这招是没用的。

网络服务器还有打开端口 139 与共享磁盘，这怎么可能呢？难道网管人员是白痴吗?! 简直是天方夜谭!!



没错！似乎是非常难以令人相信，不过小弟就真的看过这样的 Web 服务器，由于端口 139 打开又有 C 磁盘共享，根本就是打开大门欢迎你进去任意更换网页 (当然小弟当时只是逛逛，没做这件事!)，不过这类情况多半发生在一些小公司的 Web 服务器 (通常是没有专业的网管人员在管理)，所以千万不要以为端口 139 只能入侵一般的上网电脑，对于某些不重视网络安全的服务器，小兵也是能立大功的。

优点

此方式最大的优点就是进入其他 Internet 服务器就像进入你家里一般，想干什么就干什么 (更换网页、获取客户或机密数据…等)，算是对服务器进行黑客任务中最简单，也最容易的方法。

缺点

- 由于大多数的 Internet 服务器并不提供也不需要打开端口 139 与磁盘共享让其他 Windows 电脑来连接使用，因此想要找到这样的 Internet 服务器，可能不大容易。

- 即使找到了有打开端口 139 的 Internet 服务器，若该服务器并没有打开**磁盘共享**，则此方法还是没辄。

- 若遇到要键入密码，则必须要想办法破解之后才能进入，否则此方法当然无效。

- 若是该服务器中的共享磁盘都设为**只读** (Read Only)，就必须要另想他法来改为可读写，否则黑客任务就受到很大的限制，无法想干什么就干什么。

结论

由上面的几项缺点你可以看出，目前在 Internet 中你可以使用此方式入侵成功，而且尽情予取予求的服务器，多半是一些网管人员常识不足 (这样也能做网管？) 或没有网管人员的小公司或个人的网站，而通过端口 139 就可以入侵的服务器对黑客高手而言应该也没什么成就感，不过对于黑客初学者来说还是可以满足基本的黑机欲望，例如：更换该网站的主页。

有关通过端口 139 来对服务器进行黑客任务更详细的观念与原理说明与入侵一般上网电脑是完全一样的，所以请参见**黑客任务实战--个人机漏洞篇 Q4** (北京希望电子出版社)，本书中将不再讨论。

❑ 方法❷ 木马程序

木马程序是黑客任务中很重要而且很特别的一种工具，不论是初学者或是高手级黑客都爱不释手，原因无它，只要成功植入木马程序，肯定是想干什么就干什么 (当然还是要依照该木马程序所提供的功能来决定)，甚至还可进行在线监控、记录他人电脑的一举一动、获得各种机密数据、作为转向入侵或转向攻击的跳板 (Redirect Intrusion)…等，是黑客任务中最完美的表现。

优点

哈!哈! 只要成功植入的话当然就可以无所不能、无恶不做啦!

缺点

- 由于木马程序的杀伤力强大，所以许多扫毒软件都会将各类型木马程序找出来，即使成功植入，许多 Internet 服务器都有使用**防火墙** (不论软件或硬件) 或**网络监控程序**，可能会阻挡木马程序的连接 (因为使用的端口被防火墙关闭)，或是被网管人员发现异状而找出来，因此要在 Internet 服务器上成功的利用木马程序来进行黑客任务是相当不容易的。

- 即使扫毒软件或网管人员找不出你的木马程序，但也要想办法让目标服务器运行你制作好的木马程序，才可以成功植入，否则此方法也没用。

- 选择一个适当的木马程序并不容易，除了要功能强大外，最好要有自我伪装或隐藏的能力，避免被扫毒软件找到，若是能自动查看与调整所使用的端口，以避免被防火墙阻挡而无法工作则是更佳，另外还要有提供连接端口设置、端口转向…等功能，如此才能进行全方位的黑客任务。

结论

从以上的讨论中你可以发现木马程序虽然是黑客任务的重要利器，但是在实行上却有下面三大难题：

- 如何顺利的将木马 Server 程序植入 Internet 服务器中运行而且不被扫毒软件或网络防护程序找到。

- 顺利植入的木马程序如何避免被防火墙阻挡而无法正常工作或被网管人员发现而删除而失败。

- 如何选择适当且功能强大的木马程序来配合黑客任务的进行。

所以木马程序虽好，但也是成功不易啊！有关使用木马程序来