郝永清［藏锋者］ 编著

网络安全攻防实用技术深度案例分析

黑客

远程控制服务攻击技术与安全搭建实战

- 不为人知的3389攻防技术揭秘
- pcAnywhere各版本缺陷分析
- 国外最新VNC攻击技术与工具展现
- 打造实用级安全远程控制服务

科学出版社
www.sciencep.com

网络安全攻防实用技术深度案例分析

黑客远程控制服务攻击技术与安全搭建实战

郝永清［藏锋者］ 编著

科学出版社

北京

内 容 简 介

黑客对互联网上的服务器攻击，不管是基于 WEB、FTP 还是其他方式，其核心目的，都是通过普通的攻击技术，想要获取服务器的远程控制权限，进而方便、快捷地进行偷窃、攻击、欺骗等行为。从近几年的网络攻击案例比例来看，针对服务器远程控制服务的攻击正在逐步增加，有愈演愈烈的态势。同时，因为普通的网络安全管理员或者服务器所有者对新兴的远程控制服务本身的攻击比较陌生，对黑客的远程服务攻击技术不了解，进而造成很大损失。

本书独辟蹊径，以发展的眼光看待黑客攻击，紧扣远程控制服务攻防技术。书中以 Windows 系统远程终端服务（3389）、Pcanywhere、VNC 这三种国内外使用率最广的远程控制服务系统为例，辅以藏锋者网络安全（www.cangfengzhe.com）上的各种案例程序的搭建和模拟，深入分析黑客使用的密码攻击、权限攻击、漏洞攻击等方式，采取极具针对性的防范策略，构建一个安全、实用的远程控制服务器。

本书适合对网络安全技术有兴趣并想从事相关行业的大学生；就读于网络信息安全相关专业的研究生；负责企业、公司网络信息安全的从业者；网络安全技术专业研究人员；所有对网络安全有兴趣的爱好者参考阅读。

图书在版编目（CIP）数据

黑客远程控制服务攻击技术与安全搭建实战 / 郝永清编著. —北京：科学出版社，2010

（网络安全攻防实用技术深度案例分析）

ISBN 978-7-03-026271-4

Ⅰ.黑… Ⅱ.郝… Ⅲ.计算机网络–安全技术 Ⅳ. P393.08

中国版本图书馆 CIP 数据核字（2009）第 237214 号

责任编辑：田慎鹏 霍志国 / 责任校对：陈玉凤

责任印制：钱玉芬 / 封面设计：耕者设计工作室

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

骏走印刷厂印刷

科学出版社发行 各地新华书店经销

*

2010 年 1 月第 一 版 开本：787×1092 1/16

2010 年 1 月第一次印刷 印张：23

印数：1—4 000 字数：438 000

定价：49.80 元

（如有印装质量问题，我社负责调换）

作 者 简 介

郝永清 CISSP、CISP、MCSE 资深讲师，藏锋者网络安全网（www.cangfengzhe.com）核心成员之一，主要从事信息安全相关工作，负责深入分析用户安全需求；有近十年的授课经验，为 300 多家企业千余 IT 经理及 IT 技术人员做过安全培训；有丰富的项目经验，同时密切跟踪国内外的安全动态，对严重安全事件进行快速响应；对各种恶意软件进行分析，提供检测和解决方案，并完成产品的安全评估，如防火墙、入侵检测、漏洞扫描等；参与众多公司网络的渗透测试项目，并对病毒和木马有深入了解。

丛 书 序

攻防技术辩证一体

辩证的看，网络安全技术包含两个方面，正面是防御，反面是攻击，二者缺一不可：没有了攻击技术，防御技术无从谈起；没有了防御技术，攻击技术就成为摆设，没有丝毫存在的意义。

本系列书籍从始至终贯彻这一基本要点，和其他同类图书的最大区别就在于此：

我们虽然会详细模拟攻击者的攻击过程，但其目的是为了在防御的时候更加清楚的明白需要防御的“缺口”在什么地方；

我们也会详细讲解防御体系的搭建思路和过程，但是也会讨论突破这样的防御体系的新的攻击技术和思路，进而再推出适当的防御技术。

更多的时候，本系列书籍的角度是在攻击者和防御者两者之间进行切换模拟——就好比现在工作在岗位上的网络安全技术工程师一样，经常都需要扮演攻击测试者和防护者的双重身份。

贯彻始终的“黑客”思维正面导向

有圈内人曾用“妖魔化”来形容今天的黑客，很贴切但本质很荒谬、很无奈。

原本作为褒义的“黑客”一词，是指热心于计算机技术，水平高超的电脑专家。在负面新闻不明真相的炒作下，在无数恶意攻击事件的曝光之后，在利欲熏心者的盲目追崇中，目前几乎已经完全沦为贬义的破坏者的代名词。

网络需要发展，技术需要进步。让这样歪曲的思维误导的长期后果，就是越来越多的人远离“黑客”，远离本来可能为网络发展、技术进步而提供非常大助力的群体，让原本正面积极的群体变得愈加孤僻，越加“妖魔”，甚至沦陷。

所以，本系列书籍坚持正面积极的正确“黑客”思维导向，并将贯彻始终，力争明晰恶意攻击者和善意黑客之间的区别，力争将攻击技术这把锋利的刀用在推动技术进步之上，力争让更多即将误入歧途的被误导者看到光明的希望！

专注于热点技术的追踪和普及

时代在变，技术也在变，技术热点的推陈出新本质就是技术进步的演变过程。关注并专注于最新的攻防技术，并将这些新的、热的网络安全技术普及给大众，

这就是本系列书籍的重要目标之一。

就当下的网络安全状况来看，针对 Web 服务的攻防、针对服务器的渗透攻防、针对个人计算机长期精准的控制和安全、针对网络协议的缺陷研究和修补等，都是攻击者、防御者们津津乐道的话题——自然也就是本系列书籍关注的话题。

需要提出注意的是，本系列书籍是动态的，是持续变化的，是跟随着热点变化而进步的，所以本系列书籍将长期、持续的、及时地推出！

案例化和可操作性的实现尝试

就本质来说，计算机技术是一门需要动手能力比较强的学科。作为书籍来说，可操作性的优劣将决定此书的成败。

我们采用案例化的方式来进行技术讨论，针对网络安全技术的攻击和防御两方面，采用有针对性的、螺旋上升的“攻防”对立案例进行演示，力求让各技术体系毫发毕现的出现在读者面前——注意这不是空泛的理论交锋，这是可以做到“按图索骥”的一步一步攻击和防御操作的详细记录！

最大化的提升书籍的易用性

任何事情的起步都是艰辛的，作为过来人的编者深刻明白迈出第一步的艰辛，所以，对于刚刚接触网络安全相关领域的新手，对于理解书中相关概念略显吃力的读者，我们尽量将一些关键的概念以“基本概念解释”的方式贯穿在文中，并在书末提供速查表。目的只是为了提高系列书籍的易读性，让读者更能贴切的理解各种案例和操作中的原理所在。

系列书籍中，类似于“基本概念解释”的还有适当位置的“技巧”、“提示”，以及序言之后的“本书使用方法”，还有文末的基本概念速查、书中所用演示平台和工具的汇总介绍等项。

希望读者能将这些小项目利用起来，让其为深刻理解书中技术而起到应有的辅助作用。

辅助在线技术交流平台

做为人力有限的编者来说，遗漏在所难免，所以为了更好的为读者服务，也为了除了书籍之外读者还有更方便的解惑、交流、讨论平台，本书和藏锋者网络安全网（www.cangfengzhe.com）合作，由之提供在线技术交流平台，以便本系列书籍读者更快、更好、更方便的提升技术层次——当然，这个平台肯定是免费的。

部分资料来源于藏锋者

任何技术都存在表现形式上的共性，网络安全技术也不例外。正是因为存在这样的共性，在案例的选取上，本系列书籍使用了部分藏锋者网络上的相关资料。

这样做的原因一来是很多经典资料的确能很明白的说明问题，二来是因为很多典型技术的推出就是因为存在这样的典型案例，三则是出于对实用性的考虑——我们倡导的方式是读者在通读全书后，去藏锋者网站下载并搭建书中案例的相关环境，使用相关工具进行模拟攻击和模拟防护，已达到真正的将书中的技术纳为己有的目的。

纠错及感谢

编著过程仓促，难免有所遗漏或者错误，如有发现，欢迎读者使用上述的网络交流平台与编者联系，提前致谢。

在系列书籍编著过程中，得到很多藏锋者网络上的技术伙伴们的支持和帮助，在此一并感谢。

最重要的是，系列书籍的出版和推出，得到科学出版社的大力支持。特别是责任编辑田 sir，事前、事中、事后均提供了莫大的支持，鞠躬谢过。

郝永清

2009 年 9 月于北京

本书使用方法

请用虚拟机

对任何一个网络安全技术爱好者来说，虚拟机都是必须的，也是必要的。

如果读者对本书中所讲案例有兴趣，想亲手操作，已达到最佳的阅读和理解效果，请使用虚拟机在本地虚拟相关系统，并在虚拟机上使用相关工具进行攻击和防御测试。

使用虚拟机的最大目的在于保障读者自身的系统安全；

其次是为了杜绝不经意间由读者兴趣而引发的网络恶意攻击；

然后是为了读者更深刻的理解不同身份的攻击者和防御者的操作平台、操作方法和操作目的；

最后是为了读者养成网络安全技术的基本构建、调试习惯，为以后可能遇到的网络安全问题提供最基本的环境支持。

基本概念解释

文中适当位置将出现“基本概念解释”，一般情况下是对上文中和本书主题无关，但却因为案例需要而有所涉及的理论概念。

整个网络安全体系庞大到难以想象，对于有一定经验的读者来说，将文中所述技术和其他相关概念联系在一起是很有裨益的，对技术层次的提升和某方面技术的全面透彻的理解尤为重要。

对于刚刚接触网络安全技术的读者来说，直接的案例风格书籍虽然可以很方便的提高读者的操作兴趣，快速让读者获得某一领域的相关技术理解，但是未免太过于片面，太过于单调。所以，对于新手来说，“基本概念解释”将是一个比较有用的全面的理解网络安全体系的机会，有关联的相关概念更能让新手在脑中构建完整的网络安全体系图。

当然，如果是已经有深入研究的读者，阅读此书只是因为想了解其中最新的技术，那大可略过这些内容。

提示

书中适当位置将有“提示”出现，“提示”的作用是编者对特定环境和情况的

说明。

比如是为了演示这个案例而进行的非常规操作，在实际情况中不建议使用这样的操作。

简单来说“提示”就是编者因为行文需要，为了避免误导读者而做的防护措施。

技巧

和“基本概念解释”、“提示”不同，需要特别指出的是，“技巧”一般是以攻击者的角度给出的说明，这些说明一般是针对特定环境的非常有效的攻击手法。

书中可能出现为了全盘需要，模拟攻击者进行攻击的时候，没有使用最好的、最灵巧的、最直接的攻击方式，而是采用了和书中相关概念深度符合的基本手法进行攻击模拟，所以以“技巧”的方式补充说明。

案例相关工具和程序平台

网络安全技术很多时候在明白原理之后，不用自己编写相关工具，网络上已经有很多前人编写了适当的攻击和防御工具，所以“站在巨人的肩上”是最好的快速进步的法门。

书中的相关工具除了在对应的章节出现以外，还在文末有统一的附件形式速查。

另外藏锋者网络也专门为本书提供了相关工具和程序平台的下载支持，读者可以浏览并下载。

编者建议读者在虚拟机中搭建这样的相关环境，然后同样是在虚拟机中使用相关工具进行攻击模拟和防御模拟。

在线交流

为了给各技术层次的读者提供及时在线的交流平台，本书和藏锋者合作提供了一个免费的在线交流平台。

读者可以通过登录藏锋者网站（www.cangfengzhe.com）进行技术交流。

编者邮件

编著过程比较仓促，难免出错，欢迎发现错误的读者与编者联系：cangfengzhe@live.cn。

目　录

第 1 章　远程桌面（3389）攻防案例剖析

章节内容提点与概述

本章主要内容：

- ■ 远程桌面安装与使用
- ■ “.rdp” 文件分析与破解
- ■ 远程桌面暴力破解
- ■ 远程桌面（3389）密码嗅探

本章典型案例：

- □ 启用各操作系统上的远程桌面
- □ 使用 Web 页面进行远程桌面连接
- □ 渗透攻击中的 “.rdp” 文件破解
- □ 外部/内部网络中的暴力破解
- □ 远程桌面（3389）密码嗅探

本章核心概念：

● 远程桌面（Terminal Services）是从 Telnet 发展而来的一种系统自带组件，通俗地讲，它就是图形化的 Telnet，也就是说当某台服务器开启了远程桌面连接功能后，其他用户可以在网络的另一端控制这台服务器。

1.1 远程桌面（3389）组件的安装与使用

远程桌面连接是从 Windows 2000 Server 开始由微软公司提供的一个组件，该组件一经推出即受到了很多用户的拥护和喜爱，所以在 Windows XP 和 2003 中，微软公司将该组件的启用方法进行了改革，使用户通过简单的操作就可以完成在 XP 和 2003 下远程桌面连接功能的开启。

对服务器管理员来说，远程桌面作为 Windows 自身的一个优化组件，在实际的工作和管理中使用率是非常广的。不管是使用远程桌面进行日常的服务器状态监控、文件管理、安全性措施指派等，有经验的管理员都倾向于使用 Windows 自身的远程管理组件进行相关操作。

另一方面，正是因为远程桌面的高普及率，针对它的攻击也就越来越多，而且在很多攻击者的心目中，因为远程桌面本身就是一个非常优秀的高权限管理功能，所以一旦攻破远程桌面的验证系统，则意味着“一击必杀”的攻击方式达成，攻击者也就完全掌控了被攻击服务器的高级控制权限了。

本节对远程桌面组件的基本情况作了简单介绍，并以流行的 Windows 2003 Server 系统为例，演示了如何开启和关闭远程桌面组件，并且简单介绍了在 IE 中直接调用远程桌面组件进行服务器管理的方法。

后续章节将有专门的针对远程桌面组件的各种流行攻击方式实际演示，同时也有针对各种攻击方法的防御技术的实现。

1.1.1 远程桌面（3389）组件简介

说起远程桌面，普遍公认的是从 Windows 2000 Server 系统开始广泛使用的，这个说法没有任何问题。但是如果要追溯的话，实际上用户可以在 Windows 98 甚至是 DOS 系统中看到类似的身影——从根源上说，远程桌面采用的是一种类似 Telnet 的技术，它是从 Telnet 协议发展而来的。

原始的 Telnet 协议是一种 C/S 模式，客户机可以通过 Telnet 登录到高配置的服务器上，在服务器上运行程序。当程序运行时，所有的运算与存储都是交给服务器来完成的，当运算结束后，服务器才把结果反馈回客户机，这样就可以在客户机配置不够的情况下完成程序的运行工作，而且运行结果一点不慢。

> **基本概念解释：什么是 C/S？**
>
> 客户机/服务器系统（Client/Server system）简称 C/S 系统。在这个应用模式中，用户只关心完整地解决自己的应用问题，而不关心这些应用问题由系统

中哪台或哪几台计算机来完成。在 C/S 系统中，能为应用提供服务（如文件服务、打印服务、拷贝服务、图像服务、通信管理服务等）的计算机或处理器，当其被请求服务时就成为服务器。一台计算机可能提供多种服务，一个服务也可能要由多台计算机组合完成。与服务器相对，提出服务请求的计算机或处理器在当时就是客户机。从客户应用角度看，这个应用的一部分工作在客户机上完成，其他部分的工作则在（一个或多个）服务器上完成。

C/S 系统最重要的特征是：它不是一个主从环境，而是一个平等的环境，即 C/S 系统中各计算机在不同的场合既可能是客户机，也可能是服务器。C/S 系统有很多优点：用户使用简单、直观；编程、调试和维护费用低；系统内部负荷可以做到比较均衡，资源利用率较高；允许在一个客户机上运行不同计算机平台上的多种应用；系统易于扩展，可用性较好，对用户需求变动适应性好。

3389 在计算机中是指端口号，也就是 3389 端口。在一般情况下，因为 3389 端口属于 Windows 的远程桌面组件的初始端口，所以为了方便称呼，3389 一般就被用来代指远程桌面组件了。

提示：远程桌面组件的默认端口是 3389，但是 3389 端口是可以修改的，后续章节将有详细介绍。

远程桌面（Terminal Services）就是从 Telnet 发展而来的一种系统自带组件，通俗地讲，它就是图形化的 Telnet，也就是说当某台服务器开启了远程桌面连接功能后，其他用户可以在网络的另一端控制这台服务器。

基本概念解释：什么是 Telnet?

Telnet 协议是 TCP/IP 协议族中的一员，它是 Internet 远程登录服务的标准协议和主要方式，为用户提供了在本地计算机上完成远程主机工作的能力。在终端使用者的电脑上使用 Telnet 程序，用它连接到服务器。终端使用者可以在 Telnet 程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样，可以在本地就能控制服务器。

远程登录的用户通过远程桌面功能，可以实时地操作服务器，在上面安装软件，运行程序，所有的一切都像直接在本地计算机上操作一样。通过这个功能，

网络管理员可以在家中安全地控制单位的服务器，而且由于该功能是系统内置的，所以比其他第三方远程控制工具使用更方便更灵活。

1.1.2 启用各操作系统上的远程桌面

从 Windows 2000 Server 开始，各 Windows 版本的操作系统就已经附带了远程桌面的相关功能，直到今日，Windows 2000/2003/2008 等各最新版本的操作系统依然在长期地使用远程桌面组件。

下面的内容将简单介绍在各操作系统上启用远程桌面的大概步骤。

1.1.2.1 Windows 2000 Server

在 Windows 2000 系统中，Professional 版本是不能开启远程桌面功能让别人访问的，但 Server 版可以开启，但是需要安装相应的 Windows 组件。

在系统中依次指向“开始→设置→控制面板”，进入“添加/删除程序”。在“添加/删除程序”界面中选择“添加/删除 Windows 组件”，进入组件选择。

在随后出现的“添加删除 Windows 组件”窗口中，选择“终端服务”，然后单击“下一步”按钮进行安装，如图 1.1 所示。

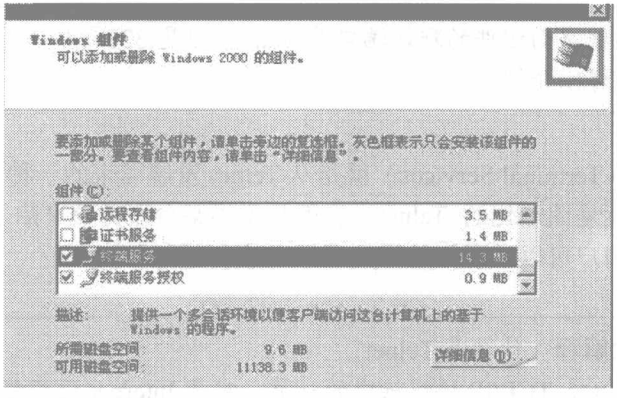

图 1.1

> **提示：**在安装过程中，可能需要插入 Windows 2000 Server 系统光盘继续安装，或者使用系统 ISO 也可。

安装完毕后需要重新启动计算机，重启后就完成了在 Windows 2000 Server 下的远程桌面连接功能的安装。

1.1.2.2　Windows XP 下启用远程桌面

在 Windows 2000 系统中引入远程桌面连接后，受到了广大用户的一致好评，但是使用者普遍认为开启该功能的方法太过复杂（对普通使用者而言），而且在使用时不能保证每个人都拥有 Windows 2000 Server 安装光盘。因此，在 Windows XP 和 Windows 2003 Server 系统中，微软将远程桌面开启的操作进行了简化。

在 Windows XP 系统下，在桌面的“我的电脑”图标上右击，选择“属性”，在弹出的系统属性窗口中选择“远程”选项卡，如图 1.2 所示。

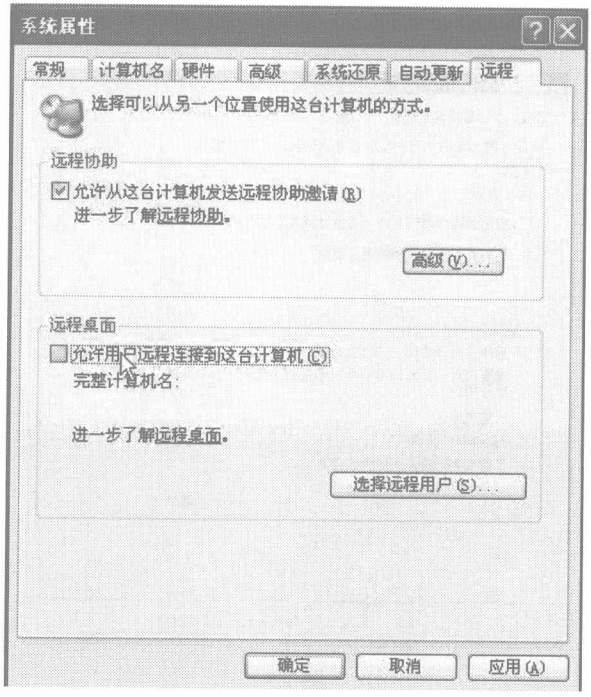

图 1.2

在上图的“远程”选项卡中找到“远程桌面”选项，选中“容许用户连接到这台计算机”复选框即可完成 Windows XP 下远程桌面连接功能的启用。

需要注意的是，因为 Windows XP 一般是给普通的个人用户使用的，所以在 XP 系统上的远程桌面默认只允许一个人在线，也就是说在默认情况下，当有远程连接发起的时候，本地系统会出现是否允许连接的提示。当本地操作用户选择了“允许”后，操作权限将移交给远程登录用户，本地操作进入锁定状态。

提示：有攻击者编写了让 Windows XP 可以同时允许两个用户同时操作而相互不影响的专用程序，有兴趣的读者可以下载试用。

1.1.2.3 Windows 2003 Server 启用远程桌面

和 Windows XP 一样，Windows 2003 Server 下开启远程桌面的方法也很简单，和 XP 系统下类似。

在 Windows 2003 Server 系统中，在“我的电脑”上右击，选择“属性”，指向“远程”选项卡，如图 1.3 所示。

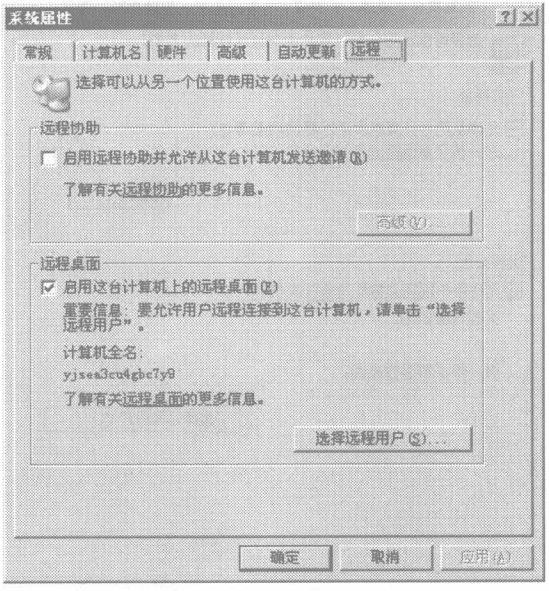

图 1.3

在上图中指向“远程桌面”，选中“启用这台计算机上的远程桌面连接”复选框，确定后即可开启远程桌面连接。

在 Windows 2003 Server 下，默认是允许有密码的管理员组的所有用户使用远程桌面连接的，如果某管理用户没有密码，是不能使用远程桌面登录的。

如果管理员想对特定的用户指派远程桌面连接权限，可以选择上图中的“选择远程用户”，进入账户选择界面，通过简单操作即可对允许连接的用户进行权限管理和指派，如图 1.4 所示。