- 探讨所有安全工作者无可回避的话题
- 揭秘网络服务器群组如何被渗透入侵
- 基于原理与实例的全面渗透防御方案
- 视频CD全程再现数十种黑客攻击战法

网络渗透攻击与安防修炼

一本内行人写给行内人的网络安全著作

- 最易被用来攻击的RFI漏洞
- 渗透网站数据库核心
- 肉鸡变跳板，端口转发
- Cisco路由器攻击案例
- 无可检测的密码后门
- SNMP威胁Windows网络安全
- 从Tomcat到3389肉鸡
- 内网中的DNS欺骗

肖　遥　编著
飞思科技产品研发中心　监制

CD-ROM
光盘包含视频教程与案例源代码

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络渗透攻击与安防修炼

网络安全专家

网络渗透攻击与安防移殊

肖　遥　编著
飞思科技产品研发中心　监制

电子工业出版社
Publishing House of Electronics Industry
北京·BEIJING

内容简介

这是一本关于网络渗透攻击与防范的书籍。全书共分为9章，主要内容包括：网络渗透攻击行为及分析、攻击者如何打开渗透突破口、渗透中的入侵与提权、远程控制入侵、大型网络环境的深入探测、渗透入侵中的社会工程学等。

本书与其他书籍不同的特色之处在于，本书特别有针对性地以曾经热炒一时的“入侵腾讯事件”为例，以再现“入侵腾讯事件”为流程，对渗透入侵过程进行了深入的分析揭秘。书中全面系统地讲解了攻击者在渗透中可能采取的各种入侵手法，并给出了高效的防范方案，有助于网络安全维护人员掌握黑客的攻击行为，更好地维护网络安全。

本书可作为专业的网络安全管理人员、网络安全技术研究者阅读，在实际工作中具有极高的参考价值；也可作为相关专业学生的学习资料和参考资料。光盘中提供攻防实战演练与视频讲解，以及书中涉及的实例源代码。

图书在版编目（CIP）数据

网络渗透攻击与安防修炼 / 肖遥编著.—北京：电子工业出版社，2009.4
（网络安全专家）
ISBN 978-7-121-08319-8

Ⅰ. 网… Ⅱ.肖… 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（2009）第 022293 号

责任编辑：王树伟　李新承
印　　刷：北京东光印刷厂
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×1092　1/16　印张：41.5　字数：1062.4 千字
印　　次：2009 年 4 月第 1 次印刷
印　　数：4 000 册　　定价：79.00 元（含光盘 1 张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

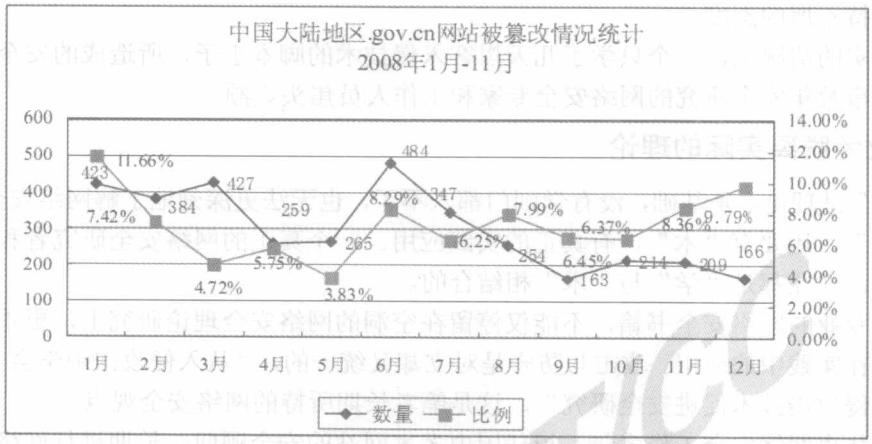
前　言

应广大读者朋友的要求，《网络渗透攻击与安防修炼》终于和广大读者见面了。这部网络安全专著分 9 章，随书附带教学视频。本书兼顾学习与参考两个目的，以广大网络管理员、安全工作者和高级网络用户为服务对象，也可供普通电脑用户了解和学习网络安全技术之用。

笔者不避寒暑，历时一载有余，三易其稿，反复修改、增删，其所追求的目标，可以概括为 6 个字：专业、深入、权威。

挑战与危机

近几年来，随着网络应用的飞速发展，各种网络攻击事件也层出不穷，对网络管理员和网络安全工作者提出了更高的要求。以“国家计算机网络应急技术处理协调中心（CNCERT）”于 2008 年底发布的网站攻击统计表为例，在 2008 年 1 月至 12 月，中国大陆地区.gov.cn 网站被篡改数量各月累计达 3595 次，其中不重复的即有 2891 个。



针对网站的攻击是明显的、易于统计的，但是针对网络进行的综合渗透攻击事件相对则要隐蔽得多，统计也不容易，因此也未能像其他网络攻击事件一样引起广泛重视。事实上，渗透攻击的发生率和危害性远远大于普通的网络攻击事件。许多网络被渗透入侵长期控制，造成大量机密信息泄露和巨额经济损失。

网络渗透攻击事件的发生极为普遍，众多的网络管理员和网络安全工作者却对网络安全环境所面临的严峻考验缺乏足够的认识，因而也未曾采取全面的防范补救措施应对各种攻击行为。

入侵腾讯事件，暴露“学”与“术”的误区

目前，市面上关于网络入侵与安全防护的书籍已经非常多了，其中不乏许多资深安全专家的精品之作。同时，有越来越多从事网络安全的管理人员和工作者，开始认识到所面临的网络安全危机，积极参加各种安全培训与认证考试。然而，许多安全书籍和各种认证培训，往往都走入了一个不易察觉的误区。

2006年轰动网络的“入侵腾讯事件”，很典型地暴露了这个误区的存在——一个年仅16岁的少年黑客，利用木马诱骗攻击入侵了著名公司腾讯的网络，控制了该公司80余台计算机的信息系统，获取了该公司的域密码及其他重要资料，进而取得多个系统数据库的超级用户权限。

作为一个国内知名的大型网络公司，其对网络安全必定极为重视。旗下众多网络安全专家及安全管理人员设置的严密安全防范措施，在一个年仅16岁的少年攻击者面前却形同虚设。不得不说，许多网络管理人员和安全工作者，对网络安全的理解与研究，往往侧重于脱离实际的理论，而对理论在现实工作中的应用则缺乏足够的认识。

目前，国内的网络安全界面临着一个非常尴尬的局面，本应该提供网络安全服务的研究组织与培训机构，却大多难以适应和满足实际工作的需求。长期以来，“学”与“术”两极分化，各执一端。

所谓“学”，是指学院式的各种网络安全理论研究，而“术”则是指实用性的技术、方法与手段。其中，“术”的最直接体现，就是各种黑客入侵攻击技术。在许多安全研究者和工作人员的眼中，往往厚“学”而薄“术”，甚至瞧不起“术”，对各种入侵行为和入侵技术持不屑的态度。

但现实的情况是，一个只学了几天黑客入侵技术的脚本小子，所造成的安全破坏，往往会让从事数年安全研究的网络安全专家和工作人员焦头烂额。

专业≠脱离实际的理论

“学”是理论，是基础，没有学则门都入不了，也无法更深刻地了解网络安全的本质；有了“学”，还要有“术”，有真正的实践应用。一个真正的网络安全研究者和合格的安全工作者，往往都是“学”与“术”相结合的。

一本专业的网络安全书籍，不能仅停留在空洞的网络安全理论研究上，更重要的是体现于理论在实践中的应用。攻击与防守是对立却又统一的，“从入侵攻击中学会安全防守，以黑客入侵攻击技术促进安全研究”，这是笔者长期所持的网络安全观点。

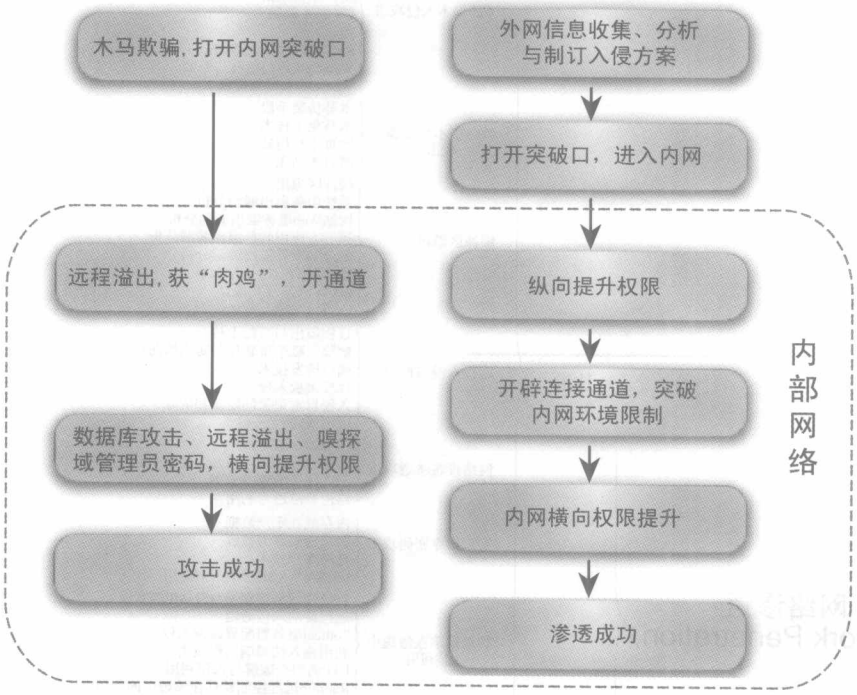
笔者从事网络安全工作多年，担任国内多家网站的安全顾问，长期进行网络渗透测试与网络风险评估。在实际的工作过程中，笔者深知国内网络环境存在着很多漏洞，也了解到部分网络安全从业人员因忽视对黑客入侵攻击事件的关注和研究，在技术上往往存在较大不足。

本书从实际应用出发，通过详细讲解攻击者习惯采用的各种渗透攻击手段与方法，揭露出网络中广泛存在，却总被忽视的安全漏洞，并结合笔者长期积累的安全防护经验，指出相应的防范要点。本书具备较强的专业性和针对性，在网络安全工作中极具参考意义和实用价值。

深入揭秘入侵事件真相

为了尽可能深入地讲解各种网络渗透攻击与测试方法，笔者特意对曾经热炒一时的“入侵腾讯事件”进行深入分析，以此类入侵流程贯穿全书，并针对攻击者每一步入侵提供各种衍生攻击手法与安全防范方案，从而使本书对网络安全工作具有极高的可借鉴性。

本书在编著过程中，力求做到原理清晰、透彻，内容全面、深入，并为本书制作了配套教学视频，整理出部分程序代码，以帮助读者真正深入地掌握渗透攻击及防范技术。



以“腾讯入侵事件”为主线展现渗透入侵攻击流程

权威、全面的知识体系

随着技术发展，网络安全越来越依赖于整体防护。与此同时，网络结构越来越复杂，攻击者入侵网络的手法也不再单一，逐步渗透的入侵攻击技术与行为已经成为主流。而常见的网络安全图书往往仅针对网络入侵中的某一部分或某几部分进行介绍，因此适用面比较窄，实用价值不高。

渗透入侵技术非常隐蔽，难以检测，一旦网络中存在某个缺口，就很有可能导致整个网络的全盘崩溃。同时，渗透攻击本身又是一种高级的入侵手法，在入侵的过程中涉及普通入侵技术、特殊攻击技术和社会工程学等，是从“技术”与“人”两个层面展开的攻击。全面了解攻击者的渗透入侵行为，是维护网络安全所必需的，因此一本权威的网络安全著作要对网络渗透攻击进行深入的分析，帮助网络安全工作者了解黑客渗透攻击行为，最终更好地维护网络安全。

本书对黑客攻击中所使用到的渗透入侵技术和手段进行了全面的分析、讲解，从渗透入侵的基础开始，逐步深入到渗透入侵的各种常见及高级手法，覆盖完整、系统而严谨的安全知识体系。

本书所涵盖的渗透入侵技术体系

一本著作的完成离不开许多人的默默支持与帮助，是众人心血和汗水的结晶。本书在编写过程中，得到了来自多方面的大力支持和不同方式的关心及帮助，借此机会对他们表示诚挚的感谢。本书最终能够出版面世，首先要感谢电子工业出版社易飞思公司的策划编辑张春雨，他的帮助和指导使我受益匪浅。安全中国、黑客基地、黑鹰安全网、华夏黑客同盟、黑客组织 H.S.T 中多位给予帮助的好友，在此也一并表示感谢。还要感谢我的妻子张黎女士，她对本书同样付出了大量的心血和时间。最后，还要特别感谢的是一直给予我人生指引和教导的李老师。

由于时间仓促，本书难免存在不足之处，真诚地希望专家、学者和读者朋友们批评指正。

肖　遥

光盘资源清单

本光盘内容主要分为视频和源代码两部分，视频位于“\Video”文件夹中，源代码位于“\Code”文件夹中。

一、视频部分

- \data\Video\第 2 章\利用 Domain 进行自动化旁注攻击

一个安全的网站是如何被其他网站“陷害”的？Domain 是一个自动化的旁注攻击工具。本视频教程演示了如何利用 Domain 对一个安全性很好且没有漏洞的网站进行入侵。由于攻击者可通过入侵其他网站，绕道攻击安全的网站，所以只要在同一虚拟主机上的其他网站存在漏洞，安全的网站实际上毫无安全性可言。

- \data\Video\第 2 章\PHP X-CODE BUG SCAN 自动挖掘文件包含脚本漏洞

RFI 文件包含漏洞的情况在 PHP 程序中广泛存在，如果难以置信，不妨试试用 PHP X-CODE BUG SCAN 这个小工具，扫描一下自认为很安全的脚本程序，结果将会让人大吃一惊！

- \data\Video\第 2 章\利用 Goo 小跑堂的一次 RFI 攻击

Google 其实很危险！Google 这个最常用的搜索引擎，在黑客手中也能变成安全攻击的武器。黑客编制出一个特殊的小工具，可以自动化采集 Google 的搜索结果，最终实现自动化批量检测入侵漏洞的目的。本视频教程演示了攻击者如何利用一个叫做 Goo 小跑堂的工具，进行针对 RFI 远程文件包含漏洞的自动化攻击。

- \data\Video\第 2 章\secdrv.sys 核心驱动溢出 Webshell 提权实例

在 Windows 系统中曾经存在一个 secdrv.sys 核心驱动溢出漏洞，这个漏洞通常用于本地权限提升攻击。看看攻击者是如何在入侵了某个网站后，利用此漏洞在 Webshell 中提升权限，实现远程提权，得以入侵并控制整个网站服务器。

- \data\Video\第 2 章\木马程序加特殊壳使国内所有杀毒软件免杀实例

再厉害的杀毒软件也有软肋，让病毒、木马免杀有时其实很简单。在本视频教程中，攻击者仅仅是利用了一个不常见的加壳软件，对病毒、木马程序进行加壳处理，就让杀毒软件无法识别了。

- \data\Video\第 2 章\IE7 0day 制作网页木马过程演示

IE7 0day 是 2008 年底在网上秘密发布的一个 IE 溢出漏洞。本视频重现了漏洞始发不久，攻击者利用网络资源制作生成 IE7 0day 漏洞攻击的网页木马的全过程。

- \data\Video\第 3 章\MS08-067 远程溢出漏洞攻击演示

MS08-067 远程溢出漏洞是 2008 年曝出的危害最严重的漏洞之一。远程溢出漏洞现在并不多见，看看 MS08-067 远程溢出漏洞攻击演示，了解一下攻击者是如何从远程无声无息地控制你的电脑！

- \data\Video\第 4 章\溢出后利用 TFTP 上传木马演示

在入侵远程溢出获得 CMD Shell 后，在本地搭建一个 TFTP 服务器，可以很容易地将木马控制程序上传到被溢出的远程主机上，继续渗透入侵。

- \data\Video\第 4 章\溢出后利用 VBE 脚本上传木马演示

对于安装了防火墙的主机，可能关闭了 FTP 和 TFTP 端口，不能直接从本机上传木马服务。不过只要主机在网络中，只要写入小小的一段 VBE 脚本，就可让主机自动通过 80 端口连接网页下载，运行木马程序，百分百突破远程主机上的防火墙。

- \data\Video\第 4 章\溢出后利用批处理上传木马演示

在溢出入侵后往往可以通过转换的方法，将 EXE 文件转换成 BAT 文件，无论远程主机多 BT，一样可以成功上传。

- \data\Video\第 4 章\AIO 渗透中的简单利用演示

AIO，这个不到几十千字节的小小入侵工具，竟然包含了数十种入侵工具的功能！看看这个恐怖的小工具，是如何被攻击者在渗透入侵过程中利用。

- \data\Video\第 4 章\灰鸽子木马配置与生成

灰鸽子是国内一款大名鼎鼎的远程控制木马，虽然历经各大杀毒软件厂商的围剿，但仍然死而不僵。看看灰鸽子木马是如何被制作出来的。

- \data\Video\第 4 章\灰鸽子木马远程控制肉鸡

数据信息泄露、摄像头被偷窥。木马的危害远不止于这些，攻击者可以利用种植在你电脑中的木马，无声无息地远程控制你的一举一动。

- \data\Video\第 5 章\利用 SNMP 入侵 Cisco 路由器

不会配置 Cisco 路由器，算不上一个合格的网管。但是 Cisco 路由器的安全配置，又有多少网管能真正做到呢？看看攻击者如何利用 Cisco 路由器的 SNMP 服务，远程入侵、控制路由器，让路由器成为渗透的跳板。

- \data\Video\第 5 章\快速入侵 ADSL 宽带路由器

ADSL 宽带路由器的应用非常普遍，不过能做到安全配置的用户却非常少。攻击者只需短短几分钟，就可随意控制数十台 ADSL 宽带路由器。

- \data\Video\第 6 章\利用 LC5 破解管理员密码

LC5 是一个老牌的破解工具，不会用这个工具就算不上是一个合格的安全技术工作者。本视频教程将揭示如何利用 LC5 破解 Windows 主机管理员的密码和账号。

- \data\Video\第 6 章\利用 CA 进行账号克隆

CA 是出现最早的一款账号克隆工具，可以让你的系统中凭空多出拥有几个管理员权限的账号，然而你却无法从系统中看出任何端倪。

- \data\Video\第 7 章\Snmputil 刺探系统信息

SNMP 服务在很多主机和网络设备上都是默认开启的，它所带来的安全隐患是你无法想象的！看看攻击者如何利用 SNMP 服务，轻易获得目标主机的详细信息。

- \data\Video\第 7 章\弱口令入侵 Tomcat Web Application Manager

Tomcat 服务器常被用在 JSP 网站中，而很多 Tomcat 服务器的弱口令漏洞也是比较常见的。攻击者利用弱口令漏洞，很容易就可以上传一个 WAR 木马，从而获得整个服务器的最高控制权限。

- \data\Video\第 7 章\ImeRdp 利用输入法漏洞远程入侵终端

Windows 系统重现输入法漏洞！输入法漏洞的危害实在太大了，如今 Windows 系统中的第三方输入法漏洞再次出现。攻击者只需要利用一个小工具，就可以在远程终端登录窗口中调用第三方输入法，让原本无法利用的第三方输入成为系统的后门，随意进入远程主机。

- \data\Video\第 8 章\RawSniffer 嗅探器的使用

在渗透入侵过程中，攻击者往往会利用一些嗅探工具设下陷阱，截取内部网络的机密信息和数据。本视频教程将演示 RawSniffer 嗅探器在渗透入侵过程中的应用。

- \data\Video\第 8 章\hijack 在嗅探中的利用

hijack 是一个综合性的 ARP 欺骗工具，嗅探是其必备的功能之一，而且可在交换环境中使用。本视频教程将演示如何在交换网络中利用 hijack 进行嗅探入侵。

- \data\Video\第 8 章\hijack 进行 ARP 欺骗挂马攻击

hijack 最恐怖之处莫过于它的 ARP 欺骗挂马功能。启动这个功能，整个局域网中的所有主机，在访问任何网站时，都会被网页木马攻击！攻击者在渗透入侵中，只需采用这种攻击方法，就可间接地控制任何内网主机，危害极其巨大。

二、代码部分

- \Code\第 3 章\Blackice ICQ iss_pam1.dll remote overflow exploit.C

ISS RealSecure/BlackICE 的协议分析模块（Protocol Analysis Module，PAM）用于通过解析网络协议来执行进一步地分析和攻击检测，使用在当前所有 ISS 入侵检测产品中。ISS RealSecure/BlackICE PAM 监视 ICQ 服务器应答处理函数中存在缓冲区溢出问题，远程攻击者可以利用这个漏洞进行远程缓冲区溢出攻击，最终以 SYSTEM 进程权限在系统上执行任意指令。这个文件是基于 Blackice ICQ 的 iss_pam1.dll 模块溢出漏洞进行攻击的程序源代码。

- \Code\第 3 章\CCProxy 6.2 Telnet Proxy Ping 远程栈溢出 POC.txt

CCProxy 6.2 是最流行的国产代理服务器软件，主要用于局域网内共享宽带上网、ADSL 共享上网、专线代理共享、ISDN 代理共享、卫星代理共享、蓝牙代理共享和二级代理共享等代理上网。CCProxy 6.2 代理服务器在远程进行 Telnet 代理时，执行 Ping 命令，如果命令长度超过许可的值就会造成溢出。本文件是用于 CCProxy 6.2 Telnet Proxy Ping 远程栈溢出攻击测试的源程序代码。

- \Code\第 3 章\CCproxy 6.5 Connect BufferOverflow POC.pl

利用 CCProxy 6.5 版本的 Connect 连接进行溢出攻击的 Code。

- \Code\第 3 章\CCproxy 6.61 HTTP CONNECT 栈溢出漏洞 POC.pl

利用 CCProxy 6.61 版本的 HTTP 代理功能，在进行 Connect 连接时进行栈溢出攻击的 Code。

- \Code\第 3 章\CCproxy 6.61 HTTP CONNECT 请求栈溢出漏洞 POC.pl

另一个 CCProxy 6.61 HTTP CONNECT 溢出的 Code。

- \Code\第 3 章\CCProxy Log Remote Stack Overflow Exploit POC.c

CCProxy 日志远程溢出漏洞攻击源 Code。

- \Code\第 3 章\IIS 的 index server .ida 和.idq ISAPI 扩展远程缓冲溢出漏洞测试代码.c

经典的 IIS 服务器 IDQ 和 IDA 远程溢出漏洞攻击代码。

- \Code\第 3 章\iMail v8.05 LDAP service remote sploit by kralor.c

一个普遍存在于各种邮件服务器上的 LDAP 远程溢出攻击代码示例。

- \Code\第 3 章\IPSwitch IMail LDAP Daemon Remote Buffer Overflow Exploit .c
- \Code\第 3 章\IpSwitch IMAIL Server IMAPD Remote r00t Exploit by kcope.c
- \Code\第 3 章\IpSwitch IMAIL Server IMAPD Remote r00t Exploit by kcope.pl

以上是 3 个邮件服务器的经典溢出攻击 Code。

- \Code\第 3 章\Microsoft IIS 5 SSL exploit 溢出漏洞测试代码.c

IIS 服务器的又一个 SSL 安全连接溢出漏洞攻击 Code。

- \Code\第 3 章\MS05029 溢出工具源代码.c
- \Code\第 3 章\Ms05039 正向溢出源代码.c
- \Code\第 3 章\Serv-U 5.2 Remote Denial of Service Exploit.c
- \Code\第 3 章\Serv-U FTPD 3.x 4.x MDTM Command remote overflow.c
- \Code\第 3 章\Symantec Multiple Firewall DNS Response Denial-of-Service.c

Symantec 防火墙曾经存在的一个 DNS 拒绝服务攻击 Code。

- \Code\第 3 章\THCIISSLame 0.3 - IIS 5 SSL remote root exploit.c
- \Code\第 3 章\THCIISSLame.c
- \Code\第 3 章\WebDAV 溢出程序代码.c
- \Code\第 3 章\webdav 溢出程序源代码.c
- \Code\第 3 章\Windows Lsasrv.dll RPC [ms04011] buffer overflow Remote Exploit.C
- \Code\第 7 章\3389.vbs

在命令行下开启 3389 终端的一段代码，简洁而强大。

目　录