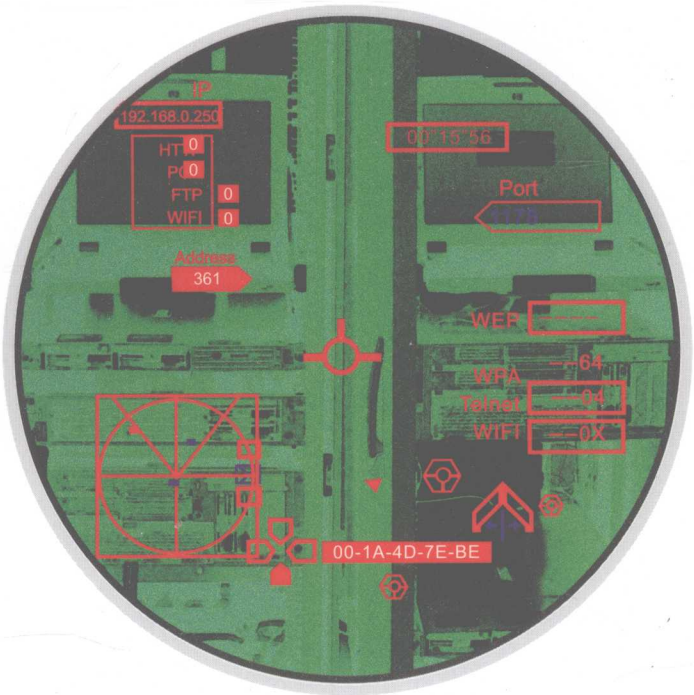
Vista/XP/2K
完全适用

WiFi 无线网络攻防战第一线实况

Hack At Will



The Bible of Hacking and AntiHacking About Windows and WiF

网络安全讲堂之全面防护

程秉辉 编著

Windows与无线网络入侵

- 船过水无痕的最佳 IP 隐藏术● WinVista、WinXP 最佳后门 Telnet 彻底全攻略
- 各种路由器、IP 分享器、无线基站、调制解调器入侵操作与彻底防护 ● 无线基站 WEP、WPA 加密密码快速破解大公开与有效防护 ● 无线基站锁定 MAC 地址、IP 地址、不公开 SSID 名称……完全突破
- 空中任意抓取无线网络数据包，各种上网资讯一览无遗 ● 黑客架设无线基站钓鱼，空中上网处处陷阱
- 快速寻找、入侵端口 139 电脑与有效防护……更多攻防密技研究与实战

清华大学出版社

网络安全讲堂之全面防护 Windows 与无线网络入侵

程秉辉　编著

清华大学出版社
北 京

内 容 简 介

本书以网络安全为线索，先分析了 Windows 与无线网络入侵的各种方式，然后再从安全防护的角度为读者构建最安全的电脑和网络。内容包括：最佳 IP 隐藏术；Windows Vista/XP 最佳后门研究；Telnet 彻底全攻略与有效防护；各种路由器、无线基站、调制解调器入侵实作与彻底防护；无线基站 WEP、WPA 加密密码快速破解大公开与有效防护；无线基站锁定 MAC 地址、IP 地址、不公开 SSID 名称等完全突破；空中任意截取无线网络数据包，各种上网信息一览无遗；黑客架设无线基站钓鱼的常用手法，空中上网处处陷阱；快速寻找、入侵打开端口 139 的计算机及其有效防护。

本书作者详细观察与记录黑客在网络中常见的各种破解与入侵行为，并提出相对应的有效防护措施，希望能帮助大家更安全、更无虑、更自在地使用网络。

本书光盘包含全球各地 IP 地址详细列表、端口列表、CurrPorts、Startup、Angry IP Scanner 、Comodo 防火墙等网管必备安全工具。

图书在版编目(CIP)数据

网络安全讲堂之全面防护 Windows 与无线网络入侵/程秉辉编著. —北京：清华大学出版社，2009.7
ISBN 978-7-302-20416-9

Ⅰ. 网…　Ⅱ. 程…　Ⅲ. ①窗口软件，Windows—安全技术②无线电通信—通信网—安全技术
Ⅳ. TP316.7　TN92

中国版本图书馆 CIP 数据核字(2009)第 097517 号

责任编辑：栾大成
封面设计：杨玉兰
版式设计：北京东方人华科技有限公司
责任校对：李玉萍
责任印制：孟凡玉
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京市清华园胶印厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×230　**印　张**：27　**字　数**：590 千字
版　　次：2009 年 7 月第 1 版　　**印　　次**：2009 年 7 月第1 次印刷
印　　数：1～6000
定　　价：49.00 元

作 者 感 言

光阴匆匆，日月如梭。笔者的《黑客任务大作战》出书至今已两三年，在市场环境如此不佳的情况下还能创造差强人意的成绩，实属难能可贵，这都归功于广大读者的大力支持。但各位读者为何要支持本书呢？是笔者的妙笔生花，还是笔者的面子够大？当然、绝对、肯定不是，应该是重视网络安全的人愈来愈多，想更进一步了解黑客的各种入侵手法——想要做黑客？No，是知己知彼才能做到有效防范，也因此让读者的书帮助更多、更广大的网民们提高网络安全意识。

时至今日，无线网络已成为许多人上网的主要方式(特别是各大城市)。虽然无线网络让大家更简单、方便地随时随地上网，但是大多数人却不知道我们目前使用的无线网络相当不安全性。**不仅WEP加密可完全破解，WPA也并非牢不可破，更可怕的是，在空中就可以任意截取他人的上网数据包**，进而取得各种有价值的资料和信息或帐户密码——无线网络几乎成为许多黑客的游戏天堂。鉴于此，我们详细地研究了黑客在无线网络中常见的各种破解与入侵行为，然后将结果详细、完全地公布在本书中，以贴近黑客思考的方式进行攻防解说，并提出相应的有效防护措施，希望能帮助大家更安全、更无虑地使用无线网络。

请填写**本书光盘中的读者服务卡**或下一页的读者资料卡，然后发送到：hawkegg@gmail.com。

请注意：本书内容完全以学理与技术实务的角度来针对有关黑客攻略与防护进行讨论与研究，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

2009.1.7

请将下表数据填妥后E-mail到**hawkegg@gmail.com**，
我们将会不定期地为您提供各种有关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://www.faqdiy.cn/**)
获取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	网络安全讲堂之全面防护Windows与无线网络入侵	本书序列号	清华出版2K90501
姓名		性别	☐先生 ☐小姐	年龄	
学历	☐研究生 ☐本科 ☐大专 ☐高中 ☐中学 ☐小学		
您的电子邮件			
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 其他：		
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
使用Windows时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：_____		
您还需要哪些方面的书籍?	☐其他Windows排困解难 ☐黑客攻防研究 ☐防黑防毒 ☐网页设计排困解难 ☐Java语言设计 ☐Windows程序设计(MFC,SDK) 其他：		
您对本书有何建议			

目 录

PART 1 入侵原理与入侵观念分析 (Basic Concepts about Hacker's Missions)..... 1

了解黑客的入侵观念..... 2
Internet 世界的基本架构..... 3
端口的角色与功能..... 5
入侵目标与攻防重点..... 11
入侵流程分析..... 14

PART 2 入侵之源——IP 隐藏术与破解 (Researches for Hiding IP Address)..... 15

Q1 黑客在进行任务时会采取哪些自我保护措施，以降低风险、避免被追查？..... 17
Q2 使用局域网上网的黑客是如何躲避网络连接设备(如路由器或防火墙)记录的？..... 17
Q3 什么情况下黑客必须隐藏自己的 IP 地址？..... 19
Q4 黑客会使用哪些方法来隐藏上网的 IP 地址？..... 19
Q5 什么是 Tor 网络？它如何突破防火墙的封锁？..... 24
Q6 黑客是如何利用 Tor 网络来达到隐藏 IP 地址的？它与跳板电脑有何不同？有何优缺点？..... 24
Q7 面对 Tor 网络与无线基站(AP)两种隐藏 IP 地址的方法，黑客如何决定与取舍？..... 24
Q8 如何让未支持代理服务器的网络软件或黑客工具也能使用 Tor 网络来隐藏 IP 地址？..... 24
Q9 如何让寄出的邮件中不包含 IP 地址？..... 33
Q10 如何让信件中包含错误 IP 地址？..... 33
Q11 为何黑客必须找出被黑者 IP 地址才可进行攻击或入侵？..... 37
Q12 黑客使用哪些方法来找出被黑者 IP 地址？..... 37
Q13 黑客是如何找出使用动态 IP 上网电脑当前的 IP 地址的？..... 37
Q14 动态 IP 上网的电脑真的比较安全吗？黑客如何猜出使用动态 IP 电脑当前上网地址？..... 37
Q15 我使用动态 IP 上网，为何还经常会被同一个黑客找到？如何防护？..... 37
Q16 黑客是如何找出特定下手目标的 IP 地址的？..... 41

Q17 黑客是如何根据地址(Address)、FTP 地址、域名(Domain Name)来找出目标的 IP 地址？ 41

PART 3 入侵目标——IP 查找与攻防(Search and Lock Target) 35

Q18 黑客是如何直接向被黑者询问出当前上网的 IP 地址的？如何防护？ 45
Q19 黑客是如何从电子邮件中找出被黑者上网 IP 地址的？如何防护？ 45
Q20 黑客是如何从网络聊天室中找出某人的 IP 地址的？如何防护？ 45
Q21 黑客是如何由实时通讯软件(如 Windows Live Messenger、Skype、雅虎通、QQ 等)找出某个好友的 IP 地址的？如何防护？ 53
Q22 对于使用动态 IP 上网的特定被黑电脑，黑客如何快速、有效地获取 IP 地址？ 57
Q23 如何防范黑客自行设计的获取被黑电脑当前上网动态 IP 地址而且不会被查杀的小工具？ 57
Q24 黑客是如何随意查找下手目标的？ 75
Q25 黑客是如何从特定的 IP 地址来快速查找出下手对象的(特别是打开端口 139 的电脑)？ 75
Q26 如何有效防止被黑客随机选定为下手的目标？ 75
Q27 黑客是如何快速找到某个公司、单位或学校中直接连接到 Internet 的电脑的，而且是使用 Windows 并打开了端口 139？如何有效防范？ 83
Q28 为什么有些网站或个人电脑的 IP 地址黑客找不到？如何实现？ 86
Q29 被黑者使用固定 IP 上网，为何黑客就是找不到？如何实现？ 86
Q30 黑客为何找不到网吧中某台电脑的 IP 地址？如何实现？ 86
Q31 某人现在就在上网，为何黑客就是找不到对方的 IP 地址？ 86
Q32 若黑客下手的目标是以虚拟 IP 或通过局域网中的其他电脑连接到 Internet，黑客会如何入侵或攻击？ 86
Q33 有什么方法可以避免一般上网电脑被黑客扫描 IP 地址或入侵？ 86

PART 4 Windows 电脑入侵分析与全面防护(Hacking and Defense for Windows Intrusion) 89

Q34 对于使用 Windows 系统上网的一般电脑，黑客会使用哪些方法进行入侵或攻击？ 91
Q35 哪些目标最适合黑客使用端口 139 入侵？ 95
Q36 黑客利用端口 139 入侵的详细流程与步骤是什么？会遇到哪些困难与麻烦？如何解决？如何产生安全思路？ 95

Q37 有些黑客可以找到许多打开端口 139 而且有磁盘共享的电脑，但有些黑客却找不到，这是什么原因？如何从中产生安全思路？ 95
Q38 如何利用 NetBrute Scanner 判断已找到的电脑所使用的 Windows 版本？ 95
Q39 黑客使用什么方法或技巧可以快速获得 Windows 的磁盘共享密码？ 133
Q40 黑客如何找出磁盘共享的电脑设置了哪些用户名？ 133
Q41 如何有效防止黑客猜中磁盘共享密码？ 133
Q42 黑客如何利用默认共享漏洞来入侵 Windows 2000/NT 电脑？ 148
Q43 每次启动 Windows 系统都会自动打开默认共享，如何始终关闭它来防止黑客入侵？ 148
Q44 被黑电脑已将默认共享彻底关闭，黑客会使用什么手段将其打开？ 148
Q45 黑客会使用哪些方法在被黑电脑中创建一个最高权限帐户？ 156
Q46 黑客会使用哪些方法打开被黑 Windows 2000/NT 电脑中的磁盘共享？ 156
Q47 黑客如何打开被黑电脑的任务计划服务，如此就可以使用 at 命令来运行程序？ 156
Q48 黑客通常会使用什么手段破解 Windows 9x/ME 电脑的磁盘共享密码？ 165
Q49 黑客利用共享密码漏洞来破解共享密码，成功率为何近 100？ 165
Q50 如何修补 Windows 9x/ME 的磁盘共享密码漏洞？ 165
Q51 黑客通过端口 139 成功入侵被黑电脑后，是如何找出各种实时通讯软件(如 Windows Live Messenger、MSN、雅虎通、QQ 等)的用户名与密码的？如何有效防护？ 173
Q52 黑客通过端口 139 成功入侵被黑电脑后，是如何找出各类帐户密码(如 ADSL 上网帐户、网络银行帐户、网络游戏帐户、Web-mail 邮箱帐户、进入某个网页的会员帐户等)的？如何有效防护？ 173
Q53 已经通过端口 139 成功入侵被黑电脑，黑客如何打开 Telnet 后门来更方便地进出？如何防范？ 186
Q54 Windows Vista 默认没有 Telnet 服务，黑客要如何安装与启动它？如何防范？ 186
Q55 对于没有提供 Telnet 服务的 Windows(如 Windows XP Home)，黑客是如何打开其 Telnet 后门的？如何防范？ 186
Q56 黑客是如何选择适合直接入侵一般上网电脑漏洞的？如何防护？ 204
Q57 黑客是如何查找利用特定漏洞来进行扫描或入侵工具的？ 204
Q58 什么是 UPnP 远程溢出入侵漏洞(MS05-039)？黑客是如何利用它入侵一般上网电脑的，且具有最高权限？为何会入侵失败？如何有效防护？ 204
Q59 如何修补 UPnP 远程溢出入侵漏洞，不让黑客利用它？ 204
Q60 黑客是如何利用路由器、无线网络无线基站或路由器调制解调器来入侵被黑电脑的？ 214
Q61 黑客是如何对一般上网的电脑进行瘫痪攻击，使其无法连接到 Internet 的？ 214

Q62 黑客是如何入侵路由器、无线网络无线基站或路由器调制解调器来偷取ADSL帐户密码的？ 214
Q63 如何有效防护黑客利用路由器、无线网络无线基站或路由器调制解调器来进行瘫痪攻击、偷取ADSL帐户密码或入侵电脑？ 214

PART 5 无线网络入侵分析与全面防护(Hacking & Antihacking about WiFi) 227

黑客可以利用无线网络做什么？ 228
可直接使用的无线网络 229
破解WEP或WPA密码 229
突破MAC地址存取限制 229
找出可使用的IP地址 229
隐藏上网IP地址 230
偷取数据包数据 230
入侵内网电脑 230
瘫痪攻击 230
Q64 黑客是如何利用无线上网来隐藏IP地址的？有何缺点？ 231
Q65 黑客是如何查找可使用的无线网络来上网的？如何让自己的无线基站不被黑客找到？ 231
Q66 为何无线网络无线基站的WEP加密密码一定可以被破解？黑客是如何进行破解的？如何防范？ 237
Q67 为何有时很快就破解出WEP加密密码，有时却要等许久？这是什么原因？黑客是如何解决的？如何产生安全思路？ 237
Q68 许多黑客都是使用Windows系统，但大多数破解WEP密码的相关工具都是在Linux系统上使用，黑客是如何简单、方便地使用运行在Linux上的工具的，且完全不影响到平常使用的Windows环境与所有磁盘？ 237
Q69 黑客是如何查找与选择最适合下手的无线网络无线基站的，且迅速破解WEP加密密码？如何防范？ 237
Q70 为什么有些网卡很快就被破解出WEP密码，有些网卡却很麻烦，甚至做不到？黑客是如何选择最适当的网卡的？ 237
Q71 黑客使用破解出来的WEP加密密码在与无线网络无线基站连接时，为何会失败？是什么原因？如何产生安全思路？ 237
Q72 有什么方法可以有效避免WEP加密密码被破解？ 237

Q73 黑客是如何破解无线网络无线基站的 WPA(或 WPA2)加密密码的？如何提高破解的概率？如何从中产生安全思路？ 264
Q74 许多黑客都是使用 Windows 系统，但方便、好用的 WPA 加密破解工具都是在 Linux 系统上使用，那么黑客是如何简单、方便地使用运行在 Linux 上的工具而完全不影响到平常使用的 Windows 环境与所有磁盘的？ 264
Q75 黑客是如何在 SpoonWpa 中选择不同的字典文件来破解 WPA 加密密码的？如何从中产生安全思路？ 264
Q76 如何有效防止 WPA 加密密码被破解？ 264
Q77 如何判断某个无线基站不会自动分配 IP 地址，需要预先在电脑中设置 IP 地址才可使用？如何从中产生安全思路？ 277
Q78 对于预先在电脑中指定 IP 地址才可使用的无线网络无线基站(即不使用 DHCP 自动分配 IP)，黑客是如何突破的？如何防范？ 277
Q79 黑客是如何快速有效地猜出无线网络无线基站允许连接使用的 IP 地址的？如何防范？ 277
Q80 黑客是如何破解 MAC 地址存取限制来使用无线网络无线基站的？如何有效防护？ 283
Q81 黑客是如何找出正在使用某个无线网络无线基站所有电脑的 MAC 地址的？如何防范？ 283
Q82 为何我的 Linux 中的 Kismet 不可用？如何让 Kismet 使用指定的无线网络设备(或网卡)？ 283
Q83 黑客是如何找出非公开无线网络无线基站名称(SSID Name)的，然后使用它？ 293
Q84 不公开的无线网络无线基站就能有效防止被他人使用吗？有什么更彻底有效的防护方法？ 293
Q85 黑客是如何截取其他电脑的无线上网数据包(802.11 Sniffer)的，然后从中分析后找出有价值的各种信息(例如各类用户名与密码、交谈内容等)？如何防范？ 301
Q86 对于有 WEP/WPA 加密的数据包，黑客是如何破解的？如何防范 301
Q87 黑客是如何从截取的数据包中快速找出有价值的信息的(如 HTTP、POP、FTP 帐户密码，MSN 好友名单，MSN 交谈内容等)？如何防范？ 301
Q88 黑客是如何实现只截取有价值信息的数据包的，其他大量而且没用的数据包都不要？如何从中产生安全思路？ 301
Q89 如何彻底有效地防止黑客从无线网络数据包中获取重要信息？ 301
Q90 黑客是如何选择最适合的无线基站来对使用该无线基站上网的电脑进行入侵的？ 334
Q91 黑客通常会使用哪些方法来入侵使用同一个无线网络无线基站中的其他电脑？如何有效防护？ 334
Q92 黑客是如何快速入侵无线网络无线基站并获取控制权的？如何有效防护？ 338
Q93 黑客成功入侵无线网络无线基站后可以获取与了解哪些信息？如何防护？ 338
Q94 黑客是如何对无线网络无线基站进行瘫痪攻击的，让所有电脑都无法上网？如何有效防护？ 342

Q95 黑客是如何对使用无线网络无线基站中的某一台电脑进行瘫痪攻击的，让它无法上网？ 342
Q96 黑客是如何借力使力、利用破解 WPA 加密的工具来对无线基站或连接的电脑进行瘫痪攻击的？如何防范？ 342
Q97 黑客是如何自行架设无线网络无线基站(或伪装成某个无线网络无线基站，Spoofing)来诱骗被黑者上网后进行各种黑客工作的？如何提高警觉？ 349
Q98 黑客会使用什么方法来提高被黑电脑使用黑客自己架设的无线基站的概率？如何防范？ 349
Q99 黑客利用无线网络无线基站钓鱼都是进行哪些工作？如何有效防范？ 349
Q100 黑客是如何利用伪装的无线基站来简单、方便地获取被黑电脑数据包信息的？如何提高警觉？ 355
Q101 使用无线基站钓鱼来截取网络数据包与在空中随意截取网络数据包有何不同？ 355
附录 1 全球各地 IP 地址详细列表 360
附录 2 端口列表 361
附录 3 CurrPorts 362
附录 4 NetStumbler 363
附录 5 Startup 364
附录 6 Tor 网络 365
附录 7 FreeCap 366
附录 8 SetupFactory 367
附录 9 NetInfo 368
附录 10 Angry IP Scanner 369
附录 11 TaskInfo 370
附录 12 各类密码寻回工具 373
附录 13 流光(Fluxay) 374
附录 14 Comodo 防火墙 376
附录 15 tftp32 377
附录 16 NetBrute Scanner 379
附录 17 Pqwak 380
附录 18 选择可用网页空间 381
附录 19 获取多媒体文件地址 383
附录 20 XN Resource Editor 386
附录 21 SuperScan 388
附录 22 X-Scan 389
附录 23 WireShark 390

附录 24　ADSL 密码终结者 391
附录 25　简单、方便、好用的 BackTrack Linux 环境 392
附录 26　下载与安装 SpoonWpa、SpoonWep2 400
附录 27　SMAC 403
附录 28　Cain & Abel 404
附录 29　net 命令说明 405
附录 30　at 命令说明 413

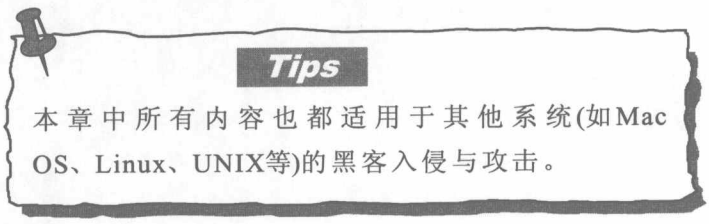
PART 1

入侵原理与入侵观念分析

Basic Concepts about Hacker's Missions

黑客任务实战系列书籍主要讲述有关黑客攻防的详细操作，市面上罕见，因此得到两岸三地不少读者的支持与鼓励。我们也收到许多读者反映的各种问题与意见，其中发现仍然有许多的读者(特别是初学者)对于黑客入侵的观念相当不正确，甚至完全没有概念，经常提出一些让笔者哭笑不得的问题。所以在本章中将详细地帮你了解正确的黑客入侵观念、Internet 世界的架构和入侵的原理与方式；从防护的角度来看，也必须彻底了解这些观念与内容，如此才可对症下药，有效阻挡黑客的入侵与攻击。

由于本章是为新读者 (特别是对黑客攻防没啥观念的人) 而写的，对于老读者或这些内容很了解的读者则说声抱歉，请从 **Part 2** 开始阅读本书。



✎ 了解黑客的入侵观念

我扫描到某个电脑打开了端口 139，为什么无法进入?
某个服务器已打开端口 80，黑客要如何入侵?
黑客有什么方法一定可以入侵某台电脑中?
有什么工具或方法一定可以获取进入某台电脑或破解某个密码?
为什么试了许久都无法破解进入某台电脑或网站的密码?
木马已经成功植入被黑电脑中，为何一直无法连接?

……

相信有基本网络概念的读者一定会觉得这些问题有点不可思议，如果只是打开某些端口就可轻易进入该电脑，那谁还敢上 Internet 啊? 相信黑客自己也不敢吧! 怎么能有入侵某电脑或破解密码的方法呢? 如果真的能这样，那 Windows 还能用吗? Bill 老大还有脸要大家继续交税吗?

答案当然是否定的，虽然许多黑客的入侵或攻击没有想象中的困难，但也并非如反掌折枝那么容易就可以完成，更不是一定可以入侵某个网站、电脑或破解密码。这种 100%成

功的做法或工具，如果真有的话，那 Internet 世界早就不存在了。这是个非常简单的逻辑，所以请各位读者不要再问笔者这种逻辑上根本就无法成立的问题。

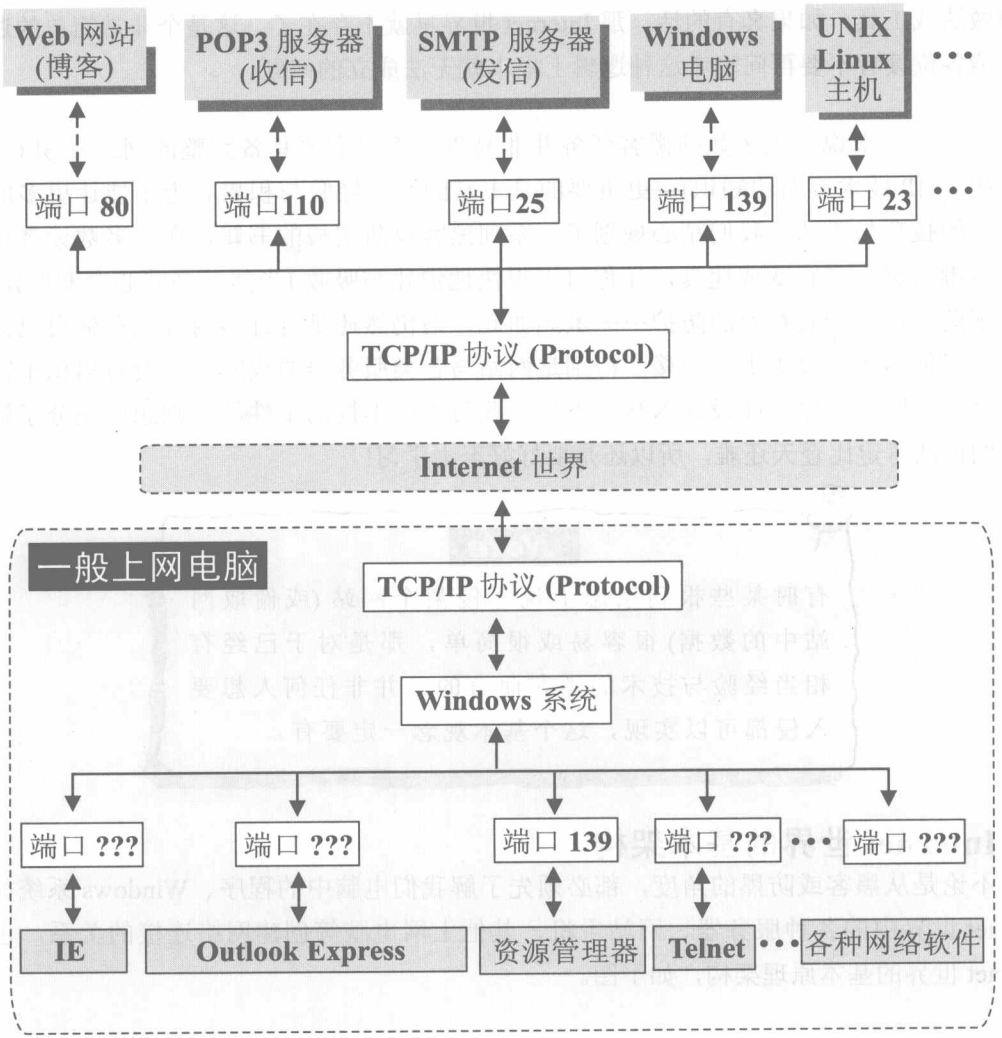
不过严格来说，大多数的黑客任务并非易事，不仅需要具备完整的网络知识 (特别是 TCP/IP 与 IP 技术方面的知识)，更重要的是丰富的实战经验与积累。为了能让更多的人了解黑客的技巧与手法，我们精心规划了一系列黑客攻防实战的书籍，在大多数读者可以了解的范围内努力将它变成速食，让你可以很快地消化与吸收 (当然不必耽心会变胖)，然后对症下药，达到彻底有效的防护……虽然如此，但仍然还是有许多内容只有你自己去努力学习与了解后才可以更上一层楼，特别是网站与各类服务器的攻防，若没有累积丰富的经验、会编写网络程序、能设计木马、不怕失败与不屈不挠的个性等，则想要充分了解黑客高手的做法肯定比登天还难，所以还是要好好努力学习!

Note

有时某些报刊杂志上说入侵某个网站 (或偷取网站中的数据) 很容易或很简单，那是对于已经有相当经验与技术的黑客而言的，并非任何人想要入侵都可以实现，这个基本观念一定要有。

✎ Internet 世界的基本架构

不论是从黑客或防黑的角度，都必须先了解我们电脑中的程序、Windows 系统如何与 Internet 世界中的各种服务器、网站主机、其他上网电脑等创建网络连接的关系，也就是 Internet 世界的基本原理架构，如下图。



从上面的图中可以清楚地看出在你的电脑中各种网络软件都是打开某一个 (或某几个) 端口再通过 Windows 系统的 TCP/IP 模块连接到 Internet 世界中的，而同样的远程服务器、网站主机或一般电脑也是以相同的方式来接收你的电脑信息 (或发送信息给你的电脑)，以此方式达成网络连接。

端口的角色与功能

由前面的图解与说明中可以看出端口是电脑进出 Internet 的大门，任何一个网络软件都只有打开一个 (或数个) 门 (端口) 之后才能与 Internet 世界沟通，连接到另一端的服务器或电脑，当任何一个网络软件退出时也必须将所打开的门 (端口) 全部关闭才行，如此才能让 Windows 系统便于管理与分配。说到这里，有些读者可能有些疑问：网络软件如何决定打开哪些端口呢? 为什么浏览网页要使用端口 80、收信服务器 POP 要使用端口 110？这是如何决定出来的? 下面就逐一来与你说明。

如何决定端口?

一般来说，每个网络软件都可以打开任何一个端口来使用 (只要该端口号码没有其他软件在使用)，不过为了在网络连接时的畅通与避免复杂，有些网络软件 (或硬件) 就会固定使用某一个 (或数个) 端口，而大家也就遵循这些不成文的规定来进行。例如，远程网站的主机一定是使用端口 80 来与你电脑中的浏览器进行连接 (一般网页)，远程的 FTP 服务器一定是使用端口21 来与你电脑中的 FTP 客户端程序进行连接，而远程的 Telnet 服务器一定是使用端口 23 来与你电脑中的 Telnet 程序进行连接。

依照目前大多数网络软件所使用的端口，下面列出常用的几个端口供大家参考。

端　口	说　　明
端口 21	FTP 文件下载上传服务
端口 23	Telnet 主机连接服务
端口 25	SMTP 发信服务
端口 80	HTTP 网页服务
端口 110	POP3 收信服务
端口 119	NNTP 新闻讨论服务
端口 139	NetBIOS 网上邻居、资源管理器连接服务
端口 443	HTTPS SSL 加密网页服务
端口 1243, 27374	Subseven 木马程序使用

还有喔