黑客任务之账户密码与机密文件

Hacking & Antihacking about Accounts Passwords and Files

◎ 程秉辉 编著

- **邮件**骗取用户名与密码的操作技巧与防
- **钓鱼网页**的假造操作与真伪判断
- 简单、有效的**手机短信**骗取用户名与密码的方法及防护
- **Windows账户与密码**的破解、入侵与防护
- 利用**P2P软件**轻易找出他人的各种用户名、密码、机密隐私文件、MSN聊天记录、电子邮件、多媒体文件的方法与彻底防护
- 利用**搜索引擎**找出他人的各种账户与密码、重要机密或隐私资料的方法与相关防护
- 各种**登录网页**的暴力破解研究操作与防护措施
- **字典文件**的研究…选择或设计最佳的暴力破解字典文件
- **代理服务器（Proxy Server）**的快速寻找与分析判断
- **POP3收信服务器**、**Telnet服务器**与**FTP服务器**的暴力破解操作与防护

…更多攻防密技研究与实战

WINDOWS 7/ VISTA/XP/2000 完全适用

科学出版社 www.sciencep.com

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

黑客任务之账户密码与机密文件

Hacking & Antihacking about Accounts Passwords and Files

◎ 程秉辉 编著

科学出版社
www.sciencep.com

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

内 容 简 介

网络安全是目前非常热门的领域，无论是个人还是企业都越来越关注网络安全。

本书作者亲自在攻防一线，详细记录黑客在网络中常见的各种入侵行为，在本书中针对于账户密码与机密文件的网络安全，从“攻”和“防”两个不同的方面，以问题的形式，通过不同的网络安全案例，从多个角度为读者剖析了常见的入侵和反入侵的手法。使读者对账户密码与机密文件的网络安全攻防技术有较为深入的认识。

本书内容丰富、图文并茂、深入浅出，适用于对研究网络安全和对安全问题感兴趣的读者。

光盘内容为书中所用部分软件工具的安装程序。

需要本书或技术支持的读者，请与北京清河 6 号信箱（邮编：100085）发行部联系，电话：010-62978181（总机）转发行部、010-82702675（邮购），传真：010-82702698，E-mail：tbd@bhp.com.cn。

图书在版编目（CIP）数据

黑客任务之账户密码与机密文件 / 程秉辉编著. —
北京：科学出版社，2010.9
ISBN 978-7-03-028211-8

Ⅰ. ①黑… Ⅱ. ①程… Ⅲ. ①计算机网络—安全技术
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 127049 号

责任编辑：刘 芯 / 责任校对：全 卫
责任印刷：金明盛 / 封面设计：青青果园

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

北京金明盛印刷有限公司印刷
科学出版社发行 各地新华书店经销
*
2010 年 9 月第 1 版 开本：787mm×1092mm 1/16
2010 年 9 月第 1 次印刷 印张：19.75
印数：1-4 000 册 字数：456 千字

定价：38.00 元（配 1 张光盘）

作者感言

本书是小弟将黑客攻防系列重新分类后的第2本 (第1本为《黑客任务之华山论木马》)，集中了各类型的账户密码与重要、机密或隐私文件的攻防研究，特别介绍黑客是如何利用电邮、手机短信、P2P 软件与网络搜索这四种方式，在许多情况下轻而易举获得成功的。这实在是相当可怕的， 相对的也充分曝露出许多人不重视、不了解，甚至是忽略网络安全的重要性，从而造成某种程度的被伤害，甚至付出惨痛的代价，而这也是小弟不断推出此系列书的最主要的目的。希望网民们能更加注意各种网络安全，提高相关的防范与警觉，如此才能充分利用网络的便利与各种优点而不是身受其害。

另外本书虽然从电子邮件、手机短信、暴力破解、P2P 软件与网络搜索这几个方面来对各种账户密码与资料文件的攻防进行讨论与研究，不过鉴于黑客常用的手法不只这几种，特别是利用截取无线网络数据包与组合式木马来获取，然而本书篇幅有限，因此这两部分已集成在《网络安全讲堂 之 Windows 与无线网络入侵》分析及《黑客任务之华山论木马》两本书中，有兴趣的读者可以自行参考。

请填写本书光盘中的读者注册卡或
下一页的读者注册卡，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各类型账户密码与重要、机密或隐私文件的攻防进行讨论与研究，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

请将以下表数据填妥后 EMail 到 hawkegg@gmail.com
我们将会不定期地为您提供有关各种 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://www.faqdiy.cn/
获得相关的更新文件与最新信息。

若您在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。

读者服务卡 REGISTER CARD

书名	黑客任务之账户密码与机密文件	本书序列号	希望电子2K10081
姓名		性别	☐先生 ☐小姐
年龄			
学历	☐硕士 ☐本科 ☐大专 ☐高中职 ☐初中 ☐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 ☐沈阳 ☐南昌 ☐郑州 ☐杭州 ☐济南 ☐长沙 ☐长春 ☐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	☐新华书店 ☐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

第 0 章　本书导读
How to read this book?

第 1 章　账户密码攻防战——个人机
Hacking & Antihacking about Accounts and Password (Personal Computer)

Q1　黑客会使用哪些方法从一般上网电脑中获取各种类型的用户名与密码 (例如：上网账户、网络银行账户、各种网上交易账户、游戏账户、Web-Mail 邮箱账户、进入某个网页的会员账户、实时通信软件账户、Windows 登录账户、Telnet 登录账户、FTP 登录账户等)？有何特点？如何有效防护？ …… 5

Q2　一般上网电脑如何应对黑客窃取各类账户密码，并彻底有效地进行防护？ … 5

Q3　黑客如何利用电子邮件骗取被黑者的各类用户名与密码？如何有效防护？ … 9

Q4　在人们对黑客通过电子邮件骗取账户密码产生警觉后，黑客会如何提高使用此方法成功的概率？ …… 9

Q5　黑客如何假造登录网页让被黑者相信，以此提高成功获取账户密码的概率？ … 9

Q6　如何有效判断登录网页是否为假造的，避免被黑客窃取账户密码？ …… 9

Q7　什么是仿冒网页 (Phishing)？它如何演变与发展？黑客如何利用它来获取被黑者的账户密码？如何防护？ ……21

Q8　黑客如何简单、快速地假造完全相同的登录网页来获取被黑者的用户名与密码？ …… 21

Q9　黑客如何利用官方登录网页进行钓鱼来获取账户密码？ ……21

Q10　如何判断登录网页是否为仿冒网页，以防止被黑客窃取账户密码？ ……21

Q11　黑客如何采用诈骗方法获取被黑者的用户名与密码？如何有效防止与防护？ …31

Q12　黑客会使用什么方法让被黑者主动而且很快地在黑客的网页或邮件中输入用户名与密码？ ……31

Q13　对于利用手机短信服务骗取各种用户名与密码，有哪些彻底有效地防护措施？ ……31

Q14　黑客会如何快速地找出许多打开端口 139 与磁盘共享的 Windows 电脑，然后进行入侵？ ……44

Q15 黑客如何快速、轻易猜中 Windows 的磁盘共享密码 (即端口 139 连接登录账户密码)？ ……44

Q16 黑客如何找出被黑电脑中可使用共享磁盘的登录用户名？ ……44

Q17 Win 9x 或 Win ME 电脑的磁盘共享密码为何能 100% 破解？ 如何有效防护？ …44

Q18 如何有效防止黑客猜中或破解磁盘共享密码 (即端口 139 连接登录密码)？ …44

Q19 黑客如何以暴力破解方式获取路由器、无线网络、无线基站、IP 共享器或调制解调器等设备的管理者登录用户名与密码？ 如何有效防护？ ……81

Q20 黑客如何借助入侵路由器、无线网络、无线基站、IP 共享器或调制解调器来窃取 ADSL 账户密码？如何有效防护？ ……81

Q21 P2P 软件是搜索与获取所想要文件的工具，为何能获取他人的用户名与密码呢？ …… 90

Q22 黑客如何利用 P2P软件获取他人的各种账户密码的？ 如何有效防护？ ……90

Q23 黑客如何利用 P2P 软件的搜索功能快速找出他人电脑中的各种账户密码？ ……90

Q24 如何有效防止 P2P 软件将电脑中的各类重要、隐私、机密文件外泄？ ……90

Q25 从被黑电脑中取到 (不论是 P2P 软件找到或利用漏洞 、木马、端口 139 入侵) 的各种文件 (如 MS-Word 、Excel、PowerPoint、Access、PDF、ZIP、RAR 、ACE、ARJ等) 需要输入密码才可以打开，黑客会如何破解？ …… 105

Q26 有些文件的密码可用密码寻回工具找出来，有些却不行， 这是什么原因？黑客会如何进行破解？ …… 105

Q27 如何有效防止各种隐私、重要或机密文件的密码被黑客破解或猜中？ …… 105

第 2 章　账户密码攻防战——服务器
Hacking & Antihacking about Accounts and Password (Server)

Q28 黑客会使用哪些方法从各类服务器中获取各种类型的用户名与密码 (例如: 网账户、网络银行账户、各种网上交易账户、游戏账户、Web-Mail 邮箱账户、进入某个网页的会员账户、Windows 登录账户、Telnet 登录账户、FTP 登录账户、POP3 登录账户等)？ 各有何特点？ 如何有效防护？ …… 117

Q29 各类服务器如何应对黑客窃取各类账户密码，并进行彻底有效的防护？ … 117

Q30 黑客如何从登录网页破解各种用户名与密码 (例如: 聊天网站、交友网站、购物网站、游戏网站、各种 XX 会员网站等)？ …… 119

Q31 一般登录网页的用户名与密码分成哪几类？黑客如何分析与决定要下手的网页？什么样的登录网页账户黑客会放弃破解？ …… 119

Q32 黑客如何分析与挑选比较容易破解出用户名与密码的登录网页？ …… 119

Q33 黑客如何分析登录网页中输入用户名与密码的设计，以及找出表单 (Form) 中动作 (Action) 的地址，如此才能将这些资料给暴力破解工具使用？ …… 119

Q34 黑客如何破解需要输入随机认证码的账户？有何困难与麻烦？ …… 119

Q35 黑客会从各种实时通信软件 (如QQ、Windows Live Messenger、雅虎通) 的网页版进行破解吗？有何困难之处？ …… 119

Q36 如何彻底有效地防止黑客利用暴力破解法猜出从网页登录的各种用户名与密码？ …… 119

Q37 为何字典文件在暴力破解登录网页中占有举足轻重的地位？ …… 149

Q38 有些黑客使用了多个字典文件 (不论是用户名或密码) 花了许多时间却一无所获，而有的黑客只使用几个字典文件就很快地猜出某个 (或某些) 用户名与密码，为何有如此大的差异？是什么原因造成的？ …… 149

Q39 黑客如何对欲破解的各种登录网页 (如Web-Mail 或各种会员网站) 进行分析，然后选择出 (或创建) 最适合的字典文件？ …… 149

Q40 黑客如何针对欲破解的登录网页 (如Web-Mail 或各种会员网站) 来设计专属的字典文件，如此才能提高破解成功的概率？ …… 149

Q41 如何有效防止黑客利用各种字典文件猜出你的用户名与密码？ …… 149

Q42 现在网络上可任意使用 (匿名，Anonymous) 的代理服务器 (Proxy Server) 屈指可数，黑客会使用哪些方法快速查找出可使用的代理服务器？有何特点？ … 160

Q43 在许多网站上列出了很多的代理服务器，但许多都已经不可用，黑客如何快速地找出其中可以使用的？ …… 160

Q44 可与 Internet 连接的代理服务器 (Proxy Server) 并不一定就能用于登录网页的暴力破解，黑客要如何分析、判断与测试出真正可使用的代理服务器？ … 160

Q45 如何有效防止黑客通过代理服务器对登录网页进行暴力破解？ …… 160

Q46 黑客如何从 Web-Mail 登录网页破解特定人 (或任意人) 的邮箱用户名与密码？有何困难之处？ …… 174

Q47 黑客如何分析 Web-Mail 登录网页的设计，找出暴力破解工具需要使用的相关资料？ …… 174

Q48 对于无法下手的Web-Mail登录网页，黑客会改用什么方法破解？ …… 174

Q49 如何有效防止 Web-Mail 的用户名与密码被黑客破解？ …… 174

Q50 黑客如何在茫茫网海中快速地找出任意的收信服务器 (POP3 或 IMAP)？ ……184

Q51 黑客如何找出某个单位或公司的收信服务器 (POP3 或 IMAP)？ …… 184

Q52 黑客如何利用暴力破解法获取收信服务器 (POP3 或 IMAP) 中特定人 (或任意人) 的用户名与密码，如此就可以获取他人的信件？ …… 184

Q53 黑客如何测试并找出 POP3 收信服务器的登录资料，然后设置在破解工具中使用？ …… 184

Q54 如何有效防止收信服务器 (POP3 或 IMAP) 的用户名与密码被黑客破解？ … 184

Q55 黑客如何在茫茫网海中快速找出提供 Telnet 服务的电脑 (也就是 Telnet) 服务器？ …… 195

Q56 黑客如何利用暴力破解法获取 Telnet 服务器中特定人 (或任意人) 的用户名与密码后入侵？ …… 195

Q57 对于各种不同登录状况的 Telnet 服务器，黑客要如何分析后使用暴力破解？ … 195

Q58 如何有效防止 Telnet 用户名与密码被黑客破解？ …… 195

Q59 黑客如何在茫茫网海中快速找出提供 FTP 服务的电脑 (也就是 FTP 服务器)？ … 216

Q60 黑客如何利用暴力破解法获取 FTP 服务器中特定人 (或任意人) 的用户名与密码？ …… 216

Q61 黑客如何破解出 FTP 账户密码后更改某个网站的网页？ …… 216

Q62 黑客如何针对各种不同的 FTP 服务器设计或选择有效的暴力破解字典文件？ … 216

Q63 如何有效防止 FTP 用户名与密码被黑客进行暴力破解？ …… 216

Q64 黑客如何利用搜索网站或相关工具找出特定人 (或任意人) 的某个用户名与密码？ …… 227

Q65 黑客如何依照搜索结果不断调整搜索关键词来重新搜索，如此就能找到想要的信息？ …… 227

Q66 在谷歌高级搜索中只能指定搜索某几种类型的文件，黑客是如何将其更改为搜索其他种类的文件？ …… 227

Q67 搜索网站或相关工具为何会成为黑客查找他人用户名与密码的工具？ 如何有效防范？ …… 227

第 3 章　重要、机密、隐私文件攻防战

Hacking & Antihacking about Important Files, E-Mail Files and Chat logs

Q68 黑客通常使用哪些方法获取他人电脑中的各类重要、机密或隐私文件？有何特点？如何有效防护？ …… 239

Q69 黑客如何利用 P2P 共享软件获取他人电脑中的各类重要、机密、隐私文件 (如简历、通信簿、工作或作业文件、报价或商业文件等)？ …… 241

Q70 黑客有什么技巧或方法可以有效提高利用 P2P 共享软件找到他人电脑中各类重要、机密、隐私文件的概率？ 如此就不会花许多时间找到一堆没价值的文件。 …… 241

Q71 哪些条件与情况下，黑客才可能利用 P2P 共享软件找到与获取特定某人电脑中的重要、机密或隐私文件？ …… 241

Q72 如何彻底有效地防止黑客使用 P2P 共享软件获取我们电脑中的重要、机密、隐私文件？ …… 241

Q73 黑客如何利用 P2P 共享软件获取他人电脑中的各类实时通信软件 (如QQ、Windows Live Messenger 、雅虎通、Skype等) 的聊天记录文件？ …… 249

Q74 黑客如何思考与决定最佳的搜索关键词，如此才能快速有效地找出他人的聊天记录文件，而不会花了许多时间找到许多没用的文件？ …… 249

Q75 在哪些条件与情况下，黑客才可能利用 P2P 共享软件找到与获取特定电脑中的聊天记录文件？ …… 249

Q76 如何彻底有效地防止黑客使用P2P共享软件获取我们电脑中的聊天记录文件？ … 249

Q77 黑客如何利用 P2P 共享软件获取他人电脑中的各类电子邮件 (如Windows Mail、Outlook Express 、Thunderbird、FoxMail等)？ …… 261

Q78 黑客如何思考与决定最佳的搜索关键词，如此才能快速有效地找出他人电脑中的电子邮件，而不会浪费许多时间一无所获？ …… 261

Q79 在哪些条件与情况下，黑客才可能利用 P2P 共享软件找到与获取特定电脑中的电子邮件？ …… 261

Q80 如何彻底有效地防止黑客使用 P2P 共享软件获取我们电脑中的电子邮件？ … 261

Q81 黑客如何利用 P2P 共享软件获取他人电脑中的各种多媒体文件 (照片、图片或视频)？ …… 272

Q82 黑客如何思考与决定最佳的搜索关键词，然后快速有效地找出他人电脑中的多媒体文件，而不会花了许多时间找出许多非个人或隐私的多媒体文件？ … 272

Q83 在哪些条件与情况下，黑客才可能利用 P2P 共享软件找到与获取特定电脑中的多媒体文件？ …… 272

Q84 如何彻底有效地防止黑客使用 P2P 共享软件获取我们电脑中的多媒体文件？ … 272

Q85 为何利用搜索网站就能轻易地找出任意人的各种资料，甚至是重要、机密或隐私资料？ …… 279

Q86 黑客如何利用搜索代码与技巧来找出任意人 (或特定人) 的各种重要、机密或隐私资料？ …… 279

Q87 黑客如何依照搜索结果不断调整搜索关键词来重新搜索，如此就更接近所想要查找的信息？ …… 279

Q88 为何利用搜索网站或相关工具就不难找到他人的重要、机密或隐私资料？这是什么原因？如何有效防护？ …… 279

附录 A　Angry IP Scanner　/286
附录 B　NetBrute Scanner　/287
附录 C　Comodo 个人防火墙　/288
附录 D　流光 (Fluxay)　/289
附录 E　ADSL 密码终结者　/291
附录 F　Foxy　/293
附录 G　eMule　/294
附录 H　ElcomSoft 各类密码寻回工具　/295
附录 I　Access Diver　/296
附录 J　SuperScan　/298
附录 K　Brutus-AET2　/299
附录 L　Mailbag Assistant　/300
附录 M　Goolag Scanner　/301
附录 N　MailBell　/302
附录 O　Hide Folders XP　/304
附录 P　EMEditor　/306

第 0 章
本书导读

How to read this book?

黑客任务
之
账户密码与机密文件

程秉辉
黑客任务实战系列

本书是小弟将黑客攻防系列书籍全部重新分类、整理与改写后的第2本书 (第1本为**《黑客任务之华山论木马》**)，本书的重心集中在各种用户名与密码破解，还有各种重要、机密或隐私文件上的攻防，然后再依照各种黑客的手法来进行说明与防护，所以本书可以只看你有兴趣的部分 (即个别的问题)，而不必 (也不需要) 从头读到尾。只是在许多的黑客行为中都会涉及到其他方面的观念、技术与操作，然而在本书篇幅有限而且尽量不与其他书中有所重复的情况下，有些并非绝对必要的内容就请读者参考其他书籍中的说明，在本书中主要有下列这两部分：

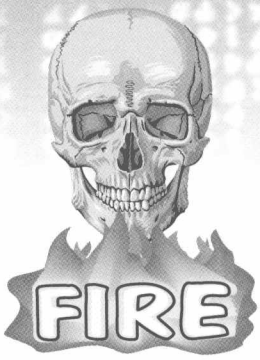
- 有关 **IP 的隐藏**请见**《网络安全讲堂之 Windows 与无线网络入侵》分析及全面防护 第2章入侵之源——IP 隐藏术与破解**。
- 有关被黑者 **IP 的查找**见**《网络安全讲堂之 Windows 与无线网络入侵》分析及全面防护第3章入侵目标——IP 查找与攻防**。

另外由于黑客对木马的使用有相当多的变化与方式，而且内容也不少，因此有关利用木马获取各类型用户名与密码，与各种重要、机密或隐私文件的操作说明与防护，都集中放在**《黑客任务之华山论木马》**一书中，有兴趣的读者可自行参考 (小弟知道有不少老读者都已经有此书，非常感谢与支持)。

第 1 章

账户密码攻防战——个人机

Hacking & Antihacking about Accounts and Password (Personal Computer)



黑客任务

之

账户密码与机密文件

程秉辉

黑客任务实战系列

黑客试图从一般上网的个人机中获取各种用户名与密码是相当常见与频繁的，最主要的原因当然是一般上网电脑不如网络服务器那般防护周密，而且有不少用户容易受骗上当，所以黑客当然乐此不疲。因此在本章中将详细与你讨论下列主题：

- 各种电子邮件的骗取手法与相关防护。
- 仿冒网页的假造方式与有效辨认。
- 手机短信的骗取手法与判断防护。
- Windows 连接登录用户名与密码的破解与彻底防护措施。
- Internet 连接的路由器、无线网络、无线基站、IP 共享器或调制解调器的管理者用户名与密码破解及有效防护。
- 利用 P2P 共享软件搜索任意人的各种用户名与密码的操作说明与彻底有效地防护方式。

Q1 黑客会使用哪些方法从一般上网电脑中获取各种类型的用户名与密码 (例如：上网账户、网络银行账户、各种网上交易账户、游戏账户、Web-Mail 邮箱账户、进入某个网页的会员账户、实时通信软件账户、Windows 登录账户、Telnet 登录账户、FTP 登录账户等)？有何特点？如何有效防护？

Q2 一般上网电脑如何应对黑客窃取各类账户密码，并彻底有效地进行防护？

相关问题请见本章中的其他问题

一般而言从用户这里下手获取各种账户密码会比从服务器端来得容易 (成功概率较高)，毕竟许多人对网络安全的警觉心还有待加强，而大多数人电脑的防护也不如服务器那样严密与安全，再加上有些账户密码一定要从用户的电脑下手才行 (例如：端口 139 或 Windows Telnet 连接账户密码、ADSL 上网账户密码等)，但这也并非毫无限制，传统上要从用户端下手必须具备下列两项条件：

- 特定的被黑者。
- 必须要能与被黑者联系，不论是电子邮件、手机、实时通信软件、聊天室、讨论区、博客、当面交谈等，否则无法对被黑者下手。

不过由于各种网络技术的发展与应用，造成如下的两种例外情况：

- 利用 P2P 软件来查找任意某个人的某个用户名与密码，如此肯定不是特定的被黑者，也不必与该被黑者联系。
- 从空中截取他人无线上网的数据包 (Data Packet)，然后从数据包中找出可能包含的用户名与密码，如此就不一定是特定的被黑者，也不必与该被黑者有所联系。

而经过多年黑客与防黑之间的争斗，黑客已经发展出许多种获取各类账户密码的方法，下面分别说明。

电子邮件骗取

虽然利用电子邮件来骗取各种进入某些网站的账户密码已经是老掉牙的招术了，不过仍然有些黑客会使此方法，反正做法简单、愿者上勾，不过为了提高成功的概率，现在许多骗取账户密码的邮件都会设计成与真正登录网页完全一样的页面，以此降低被黑者的戒心，在 **Q3** 中会有更详细深入地讨论与说明，与相对应的防护之道。

仿冒网页

其实仿冒网页基本上与邮件骗取相当类似，都是引诱被黑者到黑客设计的登录网页中输入用户名与密码来获取，其中最主要的不同之处在于技术高低，一般邮件骗取没特别的技术，只要将登录网页制作的越真实越好；而仿冒网页不一定要将登录网页设计很相像，最重要的是如何诱骗被黑者到此网页来登录，其中成功概率高低与假的登录网页地址有很大的关系，若是与真正的登录网页有相同的地址，则成功概率肯定大大增加，在 **Q7** 会进行更详细深入的研究，此处就不再说明。

心理骗取

有些黑客会利用许多人怕被占便宜 (或不愿吃亏) 的个性，发一个手机短信或邮件，告诉被黑者从本月起会从某银行账户 (或手机账单) 自动扣 xx 元的 xx 服务费 (编一个理由)，若不需要此服务或不要自动扣钱，则进入某个网站输入账户密码后就可取消此服务或自动扣款，由于与钱有关，有些人就会很快地到该网站进行验证，如此也就中了黑客的计谋，被获取用户名与密码，有关更详细地讨论、说明与有效防护请见 **Q11**。

暴力破解

所谓的暴力破解就是用**猜**的啦! 在大多数情况下都是针对服务器来进行 (例如登录各种网站的账户密码)，不过对于某些账户密码则要针对一般个人机来进行暴力破解，例如，提供端口 139 连接的电脑，也就是对 Windows 登录账户密码进行破解，更详细地操作说明与相关防护研究请详见 **Q15**。

木马获取

利用木马来获取各种登录账户密码，是从用户端下手最常见的方法之一，一般可分为使用传统木马与组合式木马，下面分别说明。

- **传统木马**。这是指一般在网络上就可获取某个 (或某一类) 账户密码的木马，由于这类木马都已公开给大家，甚至广为流传，因此几乎都已被各杀毒软件列为通缉查杀的目标，所以想要利用这类木马来成功获取各种账户密码几乎不可能，即使将木马变装易容也不见得能提高成功的概率 (可参见《**木马任务大作战**》**第2章木马伪装与破解**)，通常黑客初学者比较会使用这类木马。