“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 **93** 个问题，完整详实的告诉你各式各样的黑客任务秘技
本书 CD 包含 IP Network Browser, NeoTrace Pro, NeoLite 等多项黑客必备软件

黑客任务实战

攻略篇

北京希望电子出版社　总策划
程秉辉 John Hawke　编　写

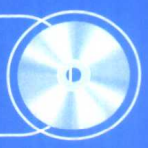
- 全球最完整的黑客攻略与操作说明
- 木马程序 SUBSEVEN 2.1、2.2 的完整操作解说
- DDoS 瘫痪攻击技术与讨论
- 如何快速有效的进行 IP 扫描
- 各类密码获取、破解技巧大公开
- 最完整的 WINDOWS 入侵和密码破解之道
- 单次／多次转向入侵（REDIRECT INTRUSION）与转向入侵的完整操作
- 如何监控他人电脑的一举一动以获取各类信息
- 最完整的黑客入侵、破坏、信息获取等行为的详细流程大公开
- 将各类木马程序、破坏程序进行伪装易容以躲避杀毒／防御软件的查杀（非合并其他软件）
- 取得他人完整邮件、截取他人邮件、账户密码破解详细实录
- 如何彻底隐藏上网 IP（连 PING 都找不到）

本书中所有内容都经过多次的严格测试，绝不告诉你无法做到的方法

中国科学出版集团
北京希望电子出版社

“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 **93** 个问题，完整详实的告诉你各式各样的黑客任务秘技
本书 CD 包含 IP Network Browser, NeoTrace Pro, NeoLite 等多项黑客必备软件



黑客任务实战

攻略篇

北京希望电子出版社 总策划
程秉辉 John Hawke 编 写

- 全球最完整的黑客攻略与操作说明
- 木马程序 Subseven 2.1、2.2 的完整操作解说
- DDoS 瘫痪攻击技术与讨论
- 如何快速有效的进行 IP 扫描
- 各类密码获取、破解技巧大公开
- 最完整的 Windows 入侵和密码破解之道
- 单次／多次转向入侵（Redirect Intrusion）与转向入侵的完整操作
- 如何监控他人电脑的一举一动以获取各类信息
- 最完整的黑客入侵、破坏、信息获取等行为的详细流程大公开
- 将各类木马程序、破坏程序进行伪装易容以躲避杀毒／防御软件的查杀（非合并其他软件）
- 取得他人完整邮件、截取他人邮件、账户密码破解详细实录
- 如何彻底隐藏上网 IP（连 Ping 都找不到）

本书中所有内容都经过多次的严格测试，绝不告诉你无法做到的方法

中国科学出版集团
北京希望电子出版社

内 容 简 介

本书以 Top-to-Down 的组织方式，直接、明了的告诉读者各种黑客入侵、破坏、信息获取方式，让你可以快速的操作，运用并进行相关的防御措施，充分达到 What you want What you got 的目的。

本书作者以完整的实战经验加上数十年的系统功力，从一般电脑使用者的角度来告诉你黑客入侵技巧、攻击、破坏、与获取信息的各种方式，你不必会写程序、也不需要了解专业的网络知识,即可轻易的按照书中的说明与操作来进行黑客任务。即可轻易的依照书中的说明与操作来进行下列各项主题的黑客任务：任务规划与工作准备，寻找与锁定目标，Windows 的入侵与攻略，木马程序实战秘技，各类黑客任务攻略，黑客任务之电子邮件，瘫痪攻击与研究。

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

本书 CD 包含 IP Network Browser, NeoTrace Pro, NeoLite 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——攻略篇
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：大成
出版、发行者：北京希望电子出版社
地　　址：北京中关村大街 26 号，100080
网　　址：www.bhp.com.cn
E-mail：lwm@hope.com.cn
电话：010-62562329，62541992，62637101，62637102，62633308，62633309
（图书发行）010-62613322-215（门市）　010-62547735（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：北京双青印刷厂
开本 / 规格：787 毫米×1092 毫米　16 开本　34 印张　616 千字
版次 / 印次：2002 年 1 月第 1 版　2002 年 1 月第 1 次印刷
印　　数：0001-5000 册
本 版 号：ISBN 7-900088-24-5
定　　价：48.00 元（本版 CD）

作者感言

所谓害人之心不可有、防人之心不可无，在 Internet 已成为大多数人生活中一部分的今日，伴随而来的黑客阴影与威胁也与日俱增，而各类型的黑客攻击事件也不断的在全球各地上演着，然而大多数个人电脑的使用者却以非常冷漠，甚至事不关己的态度来面对这些新闻，实在是相当轻忽与草率，也突显出网络安全的观念与常识的不足，随随便便运用一些简单的招数就可以找到一大堆的上网电脑来自由进出 (不论是中国、美国或日本都一样)，到他人电脑中浏览就好像逛大街一般的容易与自在。

像小弟有时随便逛逛就可以取得某些人的来往客户资料、公司资金来往状况、产品销售状况与底价、个人与家庭的隐私资料、住在那里、年龄多大、长什么样子、手机号码、与他人的往来信件、甚至某人家的狗或猫长什么样都一清二楚…特别是 Win9x 与 WinMe 的用户们，可见太多上网者的安全警觉性实在太低了，若遇到有心者入侵的话还真不知道后果会如何，这真的是非常严重的问题。

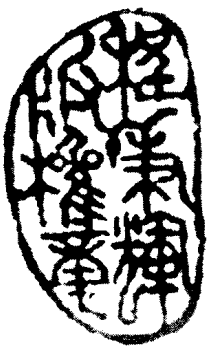
所以小弟便与 John Hawke 老兄两人抱着人饥己饥、人溺己溺、我不入地狱谁入地狱的伟大情操与精神，在全世界的上网电脑中上刀山、下油锅、无所不用其极的进行各式各样的黑客任务，然后再将这些秘技与攻略完整详实的公开给各位读者，让大家充分的了解到许多不为人知的黑客手法，并正视网络安全问题的严重性，采取相关的防御与应对措施，以保障您上网时的安全。

照例，有任何被黑客入侵的事情尽管提出来，我们一定竭尽所能的帮您解决，不过强烈建议您最好使用EMail来询问，如此我们都会尽速回覆。另外现在我们的不定期信息是以电子邮件或传真方式通知，而不再以一般邮寄方式寄送，请各位读者特别注意。

请注意：在下一页读者资料卡中的电子邮件地址请用正体写清楚，不要用草体，有些读者由于写的实在很难猜出是什么英文字母，所以就无法寄出相关讯息给您，请见谅!

请EMail到: **hawkes@ms29.hinet.net** 或 **hawke@ms16.url.com.tw**
或FAX:00-886-29189919（中国大陆读者）
FAX:001-886-2-29189919（香港读者）
FAX:当地国际电话码-886-2-29189919(其他地区读者)

请注意：本书内容完全以理论与技术的角度来针对有关黑客攻防进行讨论与研究，所以若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

目　录

第 1 章　任务规划与工作准备 (Strategies and Preparing for Hacker Mission).....1

Q1: 黑客入侵的原因或理由是什么.....3
Q2: 通常黑客是如何查找下手目标.....3
Q3: 黑客入侵、偷窃与破坏的整体流程是什么.....3
Q4: 入侵后通常有哪些攻击、破坏或偷窃行为.....3
Q5: 黑客如何隐藏自己的真正 IP 地址，不让别人追踪到.....17
Q6: 黑客要如何保护自己的 IP 地址不受到反攻击.....17
Q7: 如何使用非固定 IP 的特性来尽量避免被他人扫描或追踪.....17
Q8: 在开始查找下手对象的 IP 地址之前有哪些准备工作.....22
Q9: 为什么别人找到许多可以下手的电脑，但我扫描同一 IP 范围却很少或未找到？这是什么原因.....22
Q10: 哪些原因会造成 IP 扫描工具不可用或扫描结果不正确.....22

第 2 章　查找与锁定目标 (Search and Lock Target).....39

Q11: 如何找出特定对象的 IP 地址.....41
Q12: 如何由网址找出 IP 地址.....41
Q13: 如何找出非固定 IP 上网者当前上网 IP 地址.....46
Q14: 如何得知固定 IP 上网者的 IP 地址.....46
Q15: 如何从电子邮件中找出他人的上网 IP 地址.....46
Q16: 如何通过 ICQ 找到对方的 IP 地址.....46
Q17: 如何随意查找下手目标.....61
Q18: 如何从特定族群的 IP 地址来快速查找下手的对象.....61
Q19: 我使用 IP 扫描工具经常找了许久都没有结果，有什么快速有效的查找技巧.....61
Q20: 如何快速找到某个学校、公司或单位中连接到 Internet 的电脑，而且是运行 Windows 系统且打开端口 139.....71
Q21: 为什么有些网站或个人电脑的 IP 地址都未找到.....76
Q22: 对方明明就是使用固定 IP 上网，但为何就是未找到.....76
Q23: 某人现在就在上网，为何就是未找到 IP 地址？但我朋友却可以找到.....76
Q24: 若下手的目标是以仿真 IP 方式来连接到 Internet，并没有真正的 IP 地址，要如何入侵或攻击.....76
Q25: 我要如何知道所要下手的目标位于哪个国家或地区？怎样看到当地的地图或卫星照片.....80
Q26: 我要如何查出某个网站、FTP 服务器、DNS 服务器、某个 IP 地址…是位于哪个国家的哪个地区？怎样看到当地的地图或卫星照片.....80
Q27: 什么是端口？如何使用于黑客入侵、攻击与破坏.....87

Q28: 如何找出对方电脑打开使用的端口来进行入侵 87
Q29: 如何查找许多电脑是否打开某个特定的端口 87
Q30: 如何一次查找许多电脑打开哪些端口 87
第 3 章 Windows 的入侵与攻略 (Windows Intrusion) 97
Q31: 我要如何入侵他人电脑的 Windows 系统 99
Q32: 如何快速的找到运行 Windows 的电脑来入侵 99
Q33: 如何将有 $ 共享名的磁盘全部显示出来 99
Q34: 如何将需要输入密码的磁盘改为不用密码就可进入 120
Q35: 如何将只读的磁盘改为可读写 120
Q36: 如何破解或找出登录他人电脑的用户名与密码? 有哪些方法 129
Q37: 如何破解或找出共享密码? 可使用哪些方法 129
Q38: 遇到 NT、Win2000、WinXP 的电脑如何猜出用户名与密码 129
Q39: 如何破解只读密码将磁盘改为可读写 129
Q40: 有什么有效的方法来猜出他人电脑的用户名与密码 129
Q41: .PWL 文件中可能包含哪些密码数据 139
Q42: 如何快速找到他人电脑中的 .PWL 文件 139
Q43: 破解 .PWL 有哪些方法? 如何进行 139
Q44: 为什么有些书上的方法无法获得 .PWL 中的密码? 是什么原因 139
第 4 章 木马程序实战秘技 (Trojan Programs for Hacker Mission) 151
Q45: 为什么要使用木马程序? 它可以帮黑客做什么事 154
Q46: 如何使木马程序或 Email 给对方的破坏程序不被防御或防毒软件检测出来 157
Q47: 如何对木马程序或破坏程序进行伪装与整容 157
Q48: SubSeven、BO2K 或其他木马程序如何躲过防御或防毒软件的检测 157
Q49: 有哪些方式可以将木马程序植入他人的电脑中? 各有何优缺点 182
Q50: 哪些方式可以设置木马程序 (或其他程序) 在他人的电脑中自动运行? 各有何优缺点 191
Q51: 如何让对方立刻就可以运行植入的木马程序 (或其他程序) 191
Q52: 有什么方法可以让对方电脑立刻重启动 191
Q53: 如何快速的找出已被植入木马程序的电脑来进行各项黑客行为 199
Q54: Subseven 木马程序有哪些功能? 如何使用它来进行各种黑客任务 208
Q55: Subseven 2.2 有哪些特别的功能 208
Q56: 什么是转向入侵 (Redirect Intrusion)? 有哪些方法可做到? 各有何优缺点 267
Q57: 我要如何进行转向入侵或转向发信 267
Q58: 如何通过 2 台甚至多台电脑来进行转向入侵 267
Q59: 进行转向入侵之前有哪些需要注意与考虑的地方 267

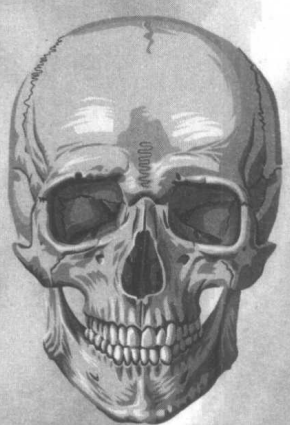
Q60: 我已经有 Proxy Server、WinGate 主机或其他个人电脑的 IP 地址可作为转向入侵，但要如何做呢？总不能使用 IE 吧.....267
Q61: 如何监控他人电脑上的各项按键操作，并将记录寄回来.....317
Q62: 如何记录他人操作电脑的画面，知道对方的一举一动.....317
Q63: 监控他人电脑的各项操作可以获得哪些重要数据.....317
Q64: 有哪些方法可以偷取网络数据包数据来进行分析？各有何优缺点.....342
Q65: 网络数据包数据可能包含哪些信息？如何破解.....342
第 5 章 各类黑客任务攻略（Hacker Attack and Operation）.....347
Q66: 有哪些方法可以偷取他人电脑中的文件？各有何优缺点.....349
Q67: 有哪些方法可以删除他人电脑中的文件或数据？各有何优缺点.....349
Q68: 如何快速找出哪些电脑打开端口 21，如此就可以使用 FTP 程序来复制与删除文件.....349
Q69: 哪些方法可以获得别人的拨号上网密码.....361
Q70: 使用他人的拨号账号上网有什么法律责任.....361
Q71: 有哪些方法可以获取他人取进入某些网站（如：FTP、各种会员、金融账户…等）的用户名与密码.....372
Q72: 如何分析获取 Cookies 文件中的用户名与密码.....372
Q73: 要使他人的电脑死机有哪些方法？各有何优缺点.....392
Q74: 有哪些方法可以将窗口炸弹送到对方电脑中.....403
Q75: 窗口炸弹对 Windows 系统有哪些破坏与影响.....403
第 6 章 黑客任务之电子邮件（Hacker Mission for E-Mail）.....411
Q76: 如何瘫痪某个电子信箱，让它无法收信.....413
Q77: 如何对某个电子信箱进行邮件炸弹攻击.....413
Q78: 如何让他人的 Outlook Express 无法收信.....413
Q79: 如何获取他人收件箱中的邮件.....427
Q80: 如何获取他人发件箱中的邮件.....427
Q81: 如何将邮件导入其他邮件箱中而不与已存在的邮件混在一起.....427
Q82: 如何截取他人还未读取的电子邮件而且不被对方发现.....439
Q83: 如何破解或获取他人电子邮件的用户名与密码？有哪些方法.....449
Q84: 如何破解或获取 Outlook Express 的用户名与密码.....449
Q85: 如何破解或获取 Web-Mail 的用户名与密码.....449
Q86: 如何对他人发黑信来恶作剧，而且对方无法知道是谁.....462
第 7 章 瘫痪攻击与研究（DDoS,Port Attack and Research）.....465
Q87: 有哪些方法可使一般电话拨号上网的电脑强迫离线？各有何缺点.....467
Q88: 什么方法可以瘫痪正在上网的个人电脑，使其无法上网甚至必须断线才行.....474
Q89: 什么叫做端口攻击？如何针对一般上网的个人电脑来进行.....474

Q90: 如何让他人无法浏览网页、无法进行 FTP 下载等 Internet 工作.....474
Q91: 什么称为 DDoS (Distributes Denial-of-Service) 攻击法.....483
Q92: 有什么方法可以瘫痪某个公司、单位、学校的服务器主机，让它工作迟缓或无法运作.....483
Q93: 如何集众人之力来瘫痪某个网站、某个邮件主机、某个服务器.....483
附录.....493
附录 A IP Network Browser.....494
附录 B NeoTrace Pro.....498
附录 C NeoLite.....500
附录 D NetBrute Scanner.....502
附录 E ICQIP.....504
附录 F PortScan 2000.....506
附录 G Angry IP Scanner.....508
附录 H SuperScan.....510
附录 I PQwak.....512
附录 J Cain.....514
附录 K ASPack.....516
附录 L IgmpNuke.....518
附录 M FakeMail.....520
附录 N Rocket.....521
附录 O SYN Flooder.....522
附录 P UPD Flooder.....523
附录 Q wwwhack.....524
附录 R IP Hacker.....525
附录 S 快猫炸慢猫.....526
附录 T Subseven.....527
附录 U EMail 杀手.....528
附录 V Norton Internet Security.....529
附录 W 文件下载专家 GetRight.....530

第1章

任务规划与工作准备

Strategies and Preparing for Hacker Mission



黑客任务实战
攻略篇
排困解难 DIY 系列

在第 1 章中我们将以 Top-to-Dwon 的流程图方式详细完整的告诉你黑客 (Hacker) 入侵、攻击与破坏的各种实战守则流程，让你充分了解黑客行为的进行方式，然后再依照其他章节中的各项黑客任务来进行，主要内容如下：

- 黑客入侵的各种目标与原因。
- 黑客行为通常有哪些?
- 如何隐藏自己的 IP 地址来避免被追踪或被对方反攻击。
- 在进行各类黑客任务之前有哪些准备工作需要注意。

Q1 黑客入侵的原因或理由是什么?

Q2 通常黑客是如何查找下手目标?

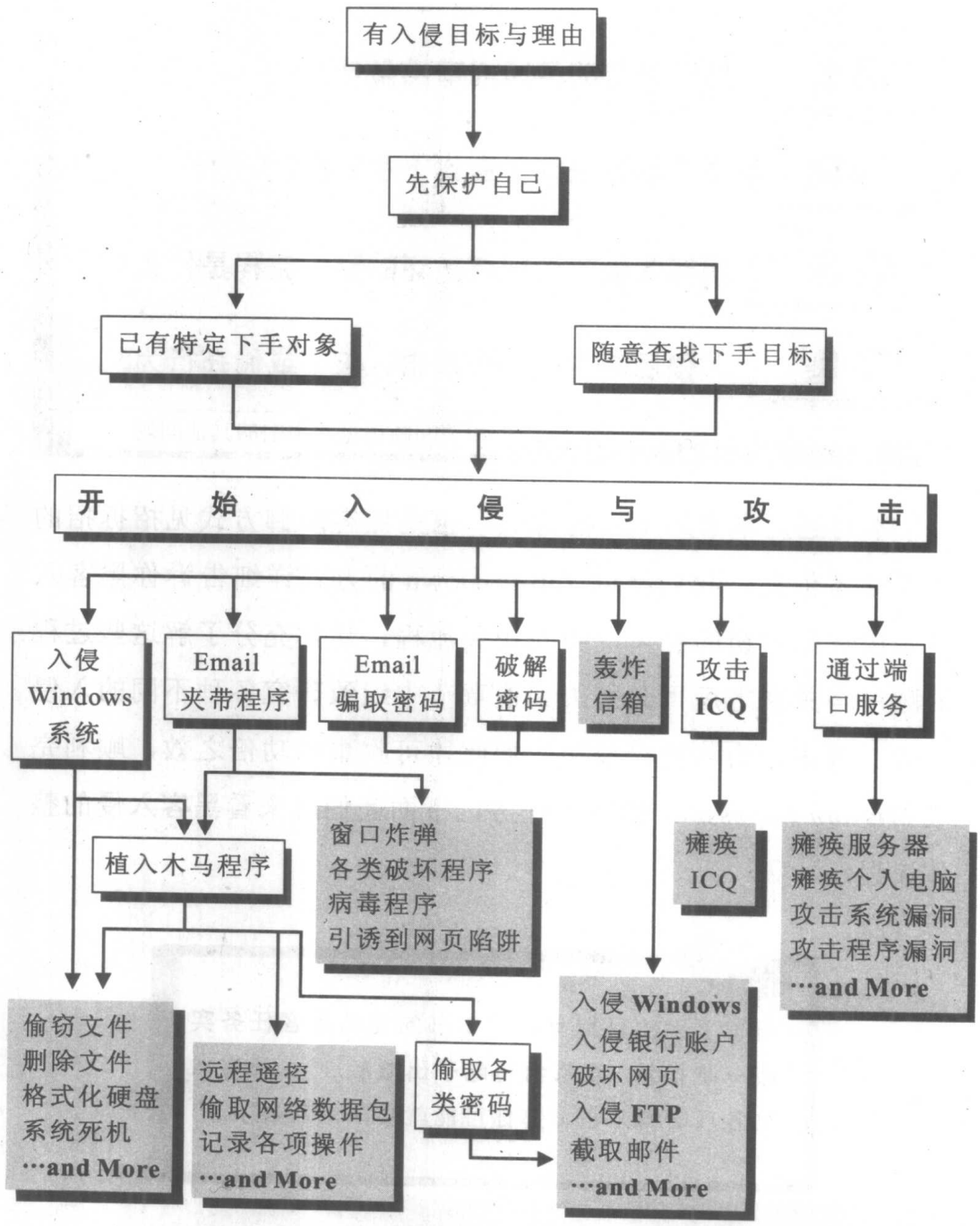
Q3 黑客入侵、偷窃与破坏的整体流程是什么?

Q4 入侵后通常有哪些攻击、破坏或偷窃行为?

相关问题请见本书中的其他问题

本问题是本书最上层的源头，也是黑客防御方式见招拆招的重要参考依据，我们将以 Top-to-Down 的方式详细告诉你黑客入侵、破坏、偷窃的整体说明与相关流程，让你充分了解这些过程的顺序与关系之后再分别去其他章节中细致研究各种不同的入侵方式、攻击行为与偷窃技巧，如此才可收事半功倍之效，顺利完成 ***Mission Impossible*** 的艰巨任务，下面我们就来看黑客入侵的整体流程。

若你下手的目标有详读本书的兄弟**黑客任务实战－防护篇（北京希望电子出版社）**，也确实做到各项防御工事，那你可能就会陷入苦战了。


有入侵目标与理由
先保护自己
已有特定下手对象
随意查找下手目标
开 始 入 侵 与 攻 击
入侵 Windows 系统
Email 夹带程序
Email 骗取密码
破解密码
轰炸信箱
攻击 ICQ
通过端口服务
植入木马程序
窗口炸弹
各类破坏程序
病毒程序
引诱到网页陷阱
瘫痪 ICQ
瘫痪服务器
瘫痪个人电脑
攻击系统漏洞
攻击程序漏洞
…and More
偷窃文件
删除文件
格式化硬盘
系统死机
…and More
远程遥控
偷取网络数据包
记录各项操作
…and More
偷取各类密码
入侵 Windows
入侵银行账户
破坏网页
入侵 FTP
截取邮件
…and More

下面我们就针对各项环节来分别进行详细的研究与讨论。

❑ 入侵目标与理由

通常黑客入侵的理由与目标不外乎下列几种原因：

- 报仇，这当然就是你不知在何时、何地得罪了某人，因此对方要藉此来讨回公道或扳回颜面，当然这样的情况下下手可能也比较狠一些，所以万事以和为贵，不要任意动气。

- 看不顺眼，以前在路上看不顺眼就动拳动刀，现在则是入侵电脑搞破坏，所以若你经常被他人看不顺眼就要特别注意了，一定要看本书的兄弟**黑客任务实战－防护篇**，以免后悔痛哭。

- 好玩、恶作剧、练功，这是许多人或学生入侵或破坏的最主要原因，除了有练功的效果外还有些许网络探险的感觉，然而此风不可长，否则一般单纯的上网用户可就累了。

- 窃取数据，可能是偷取硬盘中的文件或各种上网密码，然后从事各种商业应用、偷窃银行存款…等各种让被害者损失更大的恶行，这类黑客是最危险也是最不易发现的。

- 抗议与宣示，这是敌对国、敌对势力之间最常出现的黑客行为，大多以占领(更换)网站首页或瘫痪主机为目标，也有少部分对网

站数据进行破坏。

- 没什么特别原因或理由，想到就做。

经由以上的说明可以了解到任何一个网站与每一位上网的人都可能受到黑客的入侵与攻击，当然任何人也可能就是黑客，所以上网之前还是要有万全的准备才行!

❑ 先保护自己

做一个成功黑客的第一步就是先保护自己，否则若入侵他人不成功还被反入侵，那可真是太糗了，首先当然是要将自己的电脑环境创建如铜墙铁壁般的防御，此部分请见我们的兄弟书**黑客任务实战－防护篇**的讨论与说明，除此之外如何在作案时不被他人发现或追踪也是很重要的，下面是我们推荐的几个项目：

- 只要连接到 Internet 都会有一个 IP 地址，所以如何将真正的 IP 值隐藏起来，不被对方反追踪是很重要的，如此即使对方知道有人入侵也不容易对你进行反攻击，有关将自己上网的 IP 隐藏的各种方法请详见 **Q5** 的讨论。

- 对于入侵某些敏感的网站 (如：美国国防部 DOD、CIA、FBI、银行…等)，为了避免被这些网站的安全高手追踪，使用**转向入侵** (Redirect Intrusion) 是很重要的，特别是经过多次转向之后，

往往是追踪到不知情的代罪羔羊　而真正的黑客还不知道是躲在世界的哪个角落呢! 有关转向入侵 (Redirect Intrusion) 的详细操作与说明请见 **Q56**。

- 若你使用电子邮件作为入侵、攻击或发送相关信息的媒介，则必须将自己的电子邮件地址先隐藏起来，而且使用知名度不高而且位在国外的邮件地址，如此不仅对方追查困难而且还可以用了一次就丢掉 (不再使用)，是黑客最方便、最容易使用的工具之一。

- 就像江洋大盗要做坏事一般，总要将脸蒙住、或者易容，如此别人才不容易认出来，黑客入侵也是如此，由于现在大多数的防毒软件或各类防御程序都可以辨识出许多破坏软件或木马程序，所以对于许多无法或不愿意动手写入侵或破坏程序的黑客而言就很难完成各种偷鸡摸狗的行为（不写程序？这算什么黑客？），不过道高一尺、魔高一丈，若能对破坏软件或木马程序先进行整容，然后再送到被害者的电脑中，只要防毒软件或各类防御程序无法辨认出来，就可以开始上手了，而有关如何对破坏软件或木马程序进行整容的详细操作请见 **Q46** 的讨论。

❑ 查找下手目标

当自己的防御措施与相关准备工作都就绪之后就可以开始磨

刀霍霍向猪羊了，但是要宰哪只猪或是哪只羊呢？下面我们以已有特定对象与任意查找目标两方面来分别说明。

已有特定对象

既然已有特定的对象，则不外乎是仇家、看不顺眼、恶作剧、好玩…等原因，通常可经由下列方式来找出下手目标的门牌号号(即 IP 地址)或直接使用电子邮件地址进行入侵或攻击。

- 若入侵对象是一般上网用户，而且有固定的 IP 地址，则就可以进行入侵、攻击或其他行为，可参见下一页❑**开始入侵与攻击**中所介绍的各种方式。

- 若入侵对象是一般上网用户，但并没有固定的 IP 地址，则必须查出对方目前上网的 IP 地址后才可以进行入侵或攻击（可参考 **Q11**、**Q13** 的方法），或者是使用电子邮件地址来进行入侵或攻击，可参见下一页❑**开始入侵与攻击**中所介绍有关 Email 入侵或攻击的各种方法。

- 若入侵对象使用 ICQ，则可以通过 ICQ 来找到对方当前上网 IP 地址，然后再进行入侵或攻击，有关通过 ICQ 来找出对方 IP 地址的做法请见 **Q16** 的说明。