

## <<黑客任务大作战>>

### 图书基本信息

书名：<<黑客任务大作战>>

13位ISBN编号：9787801727022

10位ISBN编号：7801727029

出版时间：2006-9

出版时间：北京希望电子

作者：程秉辉

页数：526

字数：607000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<黑客任务大作战>>

### 内容概要

本书是从黑客的内心深处来探讨黑客的行为与做法，详细说明黑客实作的流程与步骤。全书列举143个黑客攻防实作与问题，帮您彻底了解黑客操作的各种手法，以进行有效的防护与阻挡。本书是研究黑客技术、思考想法、实际操作、心理与防护等集大成之书籍。

主要内容包括：IE漏洞入侵法、网络密码暴力破解、Windows网络入侵术、黑客IP隐身术、盗取MSN、Yahoo即时通资讯、远程溢出漏洞入侵、打开后门自由进出、简单又有效的瘫痪攻击与防护等。

书附光盘中赠送了多种系统防护、网络通信工具，以及全球各地IP地址和端口详细列表。

## <<黑客任务大作战>>

### 作者简介

程秉辉，大学毕业后无所事事、逐水草而居，精通汇编、C、WindowsAPI与Windows系统，有12年的奋斗经验与深刻了解，与微软的爱恨情仇更是生命中的转折点。从事写作至今十余年，发表过近百篇杂志文章，两岸三地共出书四十余本，Windows排困解难与黑客任务实战系列是许多读者所熟知的作品。

## <<黑客任务大作战>>

### 书籍目录

- Part 1 黑客入侵基本原理与观念 创建正确的观念 Internet 世界的基本原理 端口的角色与功能  
黑客入侵的原理与方式 黑客入侵实作流程 Part 2 IP 隐藏术与破解 Q1 黑客在进行任务时会采取哪些自我保护措施, 以降低风险避免被抓到?  
Q2 使用公司或单位网络来上网的黑客如何逃避网络连接设备 (如路由器或防火墙) 的日志追查到自己的电脑?  
Q3 什么情况下黑客必须隐藏自己的上网IP地址, 否则就有被抓到的危险?  
Q4 黑客会使用哪些方法来隐藏上网的IP地址, 不让被黑者或网管人员找到?  
Q5 黑客如何利用无线网络来隐藏 IP 地址?  
有何缺点?  
Q6 黑客如何查找可使用的无线网络来上网?  
如何让自己的无基地台不被找到?  
Q7 黑客会使用哪些方法来破解加密的无线基地台来上网?  
如何进行防护?  
Q8 黑客如何查找与使用代理服务器 (Proxy Server) 来隐藏上网IP地址?  
Q9 黑客使用代理服务器来进行黑客任务会注意那些地方? 有何优缺点?  
Q10 如何在不同的代理服务器之间来回切换使用, 降低黑客被抓到的风险?  
Q11 对于未支持代理服务器的软件, 黑客如何让它们也可以使用代理服务器来隐藏IP地址?  
Q12 如何让一般上网软件或黑客工具 (如Telnet、各种IP或漏洞扫描器、木马程序等) 也可通过HTTP代理服务器来实现隐藏IP地址?  
Q13 有些网络软件或黑客工具只能使用Socks代理服务器, 黑客如何让它们可以改用HTTP代理服务器?  
Q14 黑客会使用哪些方式不让寄出的信件中包含IP地址?  
Q15 黑客如何让信件中所包含的IP地址是无意义的, 这样就无法被追查到?  
Part 3 目标查找与锁定之攻防 Q16 为何黑客必须找出被黑者IP地址才可进行攻击或入侵?  
Q17 黑客使用哪些方法来找出被黑者IP地址?  
Q18 黑客如何找出使用动态IP电脑当前IP地址?  
Q19 动态IP上网的电脑真的比较安全吗?  
黑客如何精确找出使用动态IP电脑当前上网地址?  
Q20 我使用动态IP上网, 为何还是会经常被同一个黑客找到?  
如何防护?  
Q21 黑客如何找出特定下手目标的IP地址?  
Q22 黑客如何由网址 (Address)、FTP地址、域名称 (Domain Name) 中找出下手目标的IP地址?  
Q23 黑客如何直接向被黑者询问出当前上网的IP地址?  
如何防护?  
Q24 黑客如何从电子邮件中找出被黑者上网IP地址?  
如何防护?  
Q25 黑客如何从网络聊天室中找出某人的IP地址?  
如何防护?  
Q26 黑客如何由实时通讯软件 (如MSN、Skype、雅虎通、ICQ、QQ等) 找出某个好友的IP地址?  
如何防护?  
Q27 黑客如何随意查找下手目标?  
Q28 黑客如何从特定族群的 IP 地址来快速查找下手的对象?  
Q29 通常使用各种 IP 扫描工具都会找许久而没有结果黑客会用什么快速有效的查找技巧?  
Q30 如何有效防止被黑客随机选定为下手的目标?

## <<黑客任务大作战>>

Q31 黑客如何快速找到某个公司、单位或学校中连接到 Internet 的一般电脑，而且是使用 Windows 打开了端口 139？

Q32 为什么有些网站或个人机的 IP 地址黑客找不到？

Q33 被黑者使用固定 IP 上网，为何黑客就是找不到？

Q34 黑客为何找不到网吧中某台电脑的 IP 地址？

Q35 某人现在就在网上，为何黑客就是没法找到 IP 地址？

Q36 若黑客下手的目标是以仿真 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？

Q37 一般上网电脑有什么方法可以避免被黑客扫描 IP 地址或入侵？

Q38 黑客如何知道所要下手的目标位于哪个国家或地区？并找出详细的街道图？

Q39 黑客如何查出某个网站、某个服务器、某个 IP 地址……是在哪个国家的哪个地区？

Q40 如何找出入侵或扫描我电脑的黑客是在哪个国家或地区（并找出详细街道图）？

Q41 如何从黑客寄给我的邮件中找出对方的 IP 地址？甚至找出寄件者是位于哪个国家或哪个地区？

Part 4 Windows 入侵攻防之无孔不入 Q42 哪些目标最适合黑客使用端口 139 入侵？

Q43 黑客利用端口 139 入侵的详细流程与步骤为何？会遇到哪些困难与麻烦？如何解决？

Q44 有些黑客可以找到许多打开端口 139 的电脑，但有些黑客却找不到，这是什么原因？

Q45 若端口 139 入侵不成功，黑客还会使用哪些方法来入侵 Windows 电脑？

Q46 黑客有什么方法可以将没有共享的磁盘共享出来？

Q47 如何利用设置注册表项值就可以让被黑电脑的磁盘共享出来？

Q48 如何将需要输入密码的磁盘改为不必输入密码就可进入？

Q49 如何彻底防止黑客利用注册表项值来将电脑的磁盘设置共享？

Q50 黑客如何利用默认共享漏洞来入侵 Windows NT/2000 电脑？

Q51 每次启动进入 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？

Q52 被黑电脑已将默认共享彻底关闭，黑客会如何打开？

Q53 Windows NT/2000/XP 的用户名与密码保存在哪里？黑客如何破解它？

Q54 黑客有哪些方式或技巧比较快速、容易猜到磁盘共享密码？

Q55 黑客如何找出磁盘共享的电脑设置了哪些用户名？

Q56 如何有效防止黑客猜中磁盘共享密码？

Q57 黑客利用什么方法可有效破解 Windows 9x/ME 电脑的磁盘共享密码？

Q58 为何黑客利用共享密码漏洞来破解，成功率将近 100%？

Q59 如何修补 Windows 9x/ME 的磁盘共享密码漏洞？

Q60 若被黑电脑的磁盘只能只读（Read Only），黑客如何更改成可读写？

Q61 黑客如何在被黑的 Windows NT/2000/XP 电脑中创建最高权限账户？

Q62 如何防止共享磁盘被黑客更改成可读写？

Q63 黑客如何对 Internet 任何一台使用 Windows 的电脑发送信息吓对方？

Q64 黑客如何假冒他人名义发送信息给 Internet 上的任意 Windows 电脑？

Q65 如何让自己的电脑不再收到 Internet 上任意散发的垃圾信息？

Part 5 邮件、浏览器之入侵攻防 Q66 网页或邮件中可以包含或夹带什么东西来帮黑客进行工作？

Q67 黑客可以利用哪些方法让网页或邮件中包含或夹带的东西运行，来达到入侵或破坏的目的？如何防护？

## <<黑客任务大作战>>

Q68 黑客如何利用网页或邮件包含的程序码来修改被黑电脑中的注册表项值 ( Registry Value ) ? 可以实现哪些入侵或破坏的工作 ?

Q69 黑客如何使用网页或邮件来更改IE浏览器或Internet的各项设置 ?

Q70 黑客如何使用网页或邮件来让被黑电脑无法运行任何程序等破坏行为 ?

Q71 黑客如何诱骗被黑者运行网页或信件中包含的程序码 ?

Q72 有什么方法可以有效阻止黑客利用网页或邮件修改我电脑中的注册表项值 ?

Q73 黑客如何利用信件或网页包含的程序码来运行被黑电脑中的某个程序 ?

可以实现哪些入侵或破坏工作 ?

Q74 黑客如何利用信件或网页对被黑电脑的磁盘进行格式化 ( Format ) ?

如何设计一个格式化网页 ?

Q75 黑客如何利用信件或网页打开被黑电脑中的各种系统服务 ( 或后门 ) ?

Q76 如何有效阻挡恶意的信件或网页运行我电脑中的任何程序 ?

Q77 黑客如何想尽办法让被黑者浏览网页就可以趁机植入木马、运行被黑电脑中的程序、批处理文件或更改注册表项值 ?

Q78 黑客如何处心积虑地利用邮件或浏览器来进行入侵或破坏工作 ?

Q79 浏览器为何成为网络安全的罪魁祸首 ?

黑客如何利用它 ?

Q80 黑客如何利用人性的弱点或好奇心来更顺利地利用漏洞入侵被黑电脑 ?

Q81 什么是图片查看器处理漏洞 ( MS06-001 ) ?

黑客如何利用它 ?

如何修补 ?

Q82 如何有效防止打开某个网页就自动运行隐藏在其中的恶意源码 ( 如 : 木马、病毒程序、DOS命令、更改注册表项值等 ) ?

Q83 窗口炸弹会对 Windows 系统有哪些破坏与影响 ?

Q84 黑客为何将窗口炸弹放在 附件中, 而不直接放在HTML信件中 ?

有何优点 ?

Q85 如何避免受到窗口炸弹的攻击 ?

Q86 我受到窗口炸弹攻击, 一打开信件程序就会不断地冒出许多窗口, 无法收信与寄信, 如何解决 ?

Part 6 各类密码骗取与入侵后之攻防 Q87 黑客会使用哪些方法骗取各类账户与密码 ?

如何防护 ?

Q88 黑客会使用哪些方法破解或获取各种电子邮件账户 ( 含Web-Mail ) 的用户名与密码 ?

Q89 黑客如何随意查找收信服务器, 然后破解出某些被黑者的账户后偷看信件 ?

Q90 如何有效防止电子邮件账户的密码被黑客获取 ?

Q91 黑客如何截取被黑者还未读取的电子邮件而不被发现 ?

如何防护 ?

Q92 如何防止自己还未读取的信件被黑客偷看 ?

Q93 黑客如何破解从网页登录的电子邮件账户 ?

Q94 黑客如何破解从网页登录的各种用户名与密码 ( 例如 : 情色会员网站、聊天网站、交友网站、购物网站、XX会员网站等 ) ?

Q95 黑客通常将网页密码分为哪几类 ?

如何决定与分析要下手的网页 ?

什么样的网页密码黑客会毫不考虑地放弃破解 ?

Q96 如何彻底有效地防止黑客利用暴力破解法来猜出各种用户名与密码 ?

Q97 黑客进入被黑电脑中通常会进行哪些工作 ?

Q98 哪些文件、资料是黑客最可能的下手目标 ?

Q99 若不幸被黑客入侵, 如何有效防止重要文件被黑客偷取, 或让黑客无法打开 ?

## <<黑客任务大作战>>

- Q100 黑客如何获取与查看他人电脑中电子邮件文件中的信件？
- Q101 如何查看Outlook Express, Netscape Meeesger, Eudora, FoxMail等各种邮件程序(含不同版本)的信件文件？
- Q102 如何尽可能防止黑客获取你在电脑中保存的电子邮件？
- Q103 黑客如何查看、修改与删除他人电脑的注册表(Registry)？
- Q104 系统注册表(Registry)中哪些项值最可能会被黑客更改而要经常查看？
- Q105 如何防止黑客查看、更改或删除我的注册表(Registry)？
- Q106 Cookies文件中可能包含哪些信息？
- Q107 黑客如何分析获取Cookies文件中进入某些网站或Web-Mail的用户名与密码？
- Q108 如何有效防止黑客获取我的Cookies文件？
- Q109 黑客如何破解ZIP, RAR, ACE, ARJ等压缩文件的密码？
- 如何防护？
- Q110 黑客如何破解各版本MS-Word, Excel, PowerPoint, Access等文件的密码？
- 如何防护？
- Q111 黑客如何破解PDF文件的密码？
- 如何防护？
- Q112 黑客如何偷取各类实时信息软件(IM, 如MSN、雅虎通、ICQ、QQ)的账户、交谈日志、好友名单？
- 如何防护？
- Part 7 服务器入侵攻防战(Hacking & Antihacking for Internet Server) Q113 黑客为何要入侵或攻击各种网络服务器？
- 有啥价值？
- Q114 黑客通常会使用哪些方式入侵服务器？
- 实作流程为何？
- Q115 黑客如何在茫茫网海中快速查找提供了Telnet服务的电脑？
- Q116 黑客如何破解Telnet登录账户与密码, 然后进行入侵？
- 如何防护？
- Q117 黑客如何让一般上网的Windows电脑提供Telnet服务后进行入侵？
- Q118 如何查看我的电脑是否提供了Telnet服务？
- Q119 不论是否打开了Telnet服务, 如何防止黑客利用Telnet服务入侵我的电脑？
- Q120 黑客为何要入侵提供了FTP服务的电脑？
- 有啥价值？
- Q121 黑客如何在茫茫网海中快速查找提供了FTP服务的电脑来入侵？
- Q122 黑客如何破解登录FTP的账户与密码, 然后进行入侵或更改他人网页？
- 如何防护？
- Q123 黑客如何在茫茫网海中快速查找提供了终端机服务的Windows电脑？
- Q124 黑客如何破解登录终端机服务电脑的账户与密码, 然后进行入侵或破坏？
- Q125 黑客如何打开一般上网电脑的终端机服务后门, 然后进行远程遥控、为所欲为？
- Q126 如何更改默认的终端机端口3389来彻底有效防止黑客入侵？
- Q127 黑客如何快速查找出目标服务器有哪些漏洞(包含最新的漏洞), 然后针对这些漏洞来进行入侵或攻击？
- Q128 服务器漏洞的扫描工具有哪几种？
- 黑客要如何决定使用哪一种？
- Q129 黑客如何判断与决定要使用哪个漏洞来进行入侵或攻击？
- Q130 黑客如何快速查找某个特定漏洞的扫描工具？
- Q131 若特定漏洞的扫描工具很慢, 黑客会利用什么技巧在茫茫网海中快速地查找到任意下手的目标？

## <<黑客任务大作战>>

Q132 如何尽快修补Windows系统或Web系统（例如：IIS、Apache等）的各种漏洞，让黑客无法利用？

Q133 什么是 UPnP 远程溢出入侵漏洞（MS05-039）？  
黑客如何利用它迅速入侵网络服务器或一般电脑而且具有最高权限？

Q134 如何修补UPnP远程溢出入侵漏洞，不让黑客利用它来入侵？

Q135 一个典型的远程溢出入侵漏洞实作是如何进行的？  
有哪些原因造成有漏洞的电脑无法成功入侵？

Q136 黑客为何要让某个服务器无法提供网络服务？  
有啥价值所在？

Q137 什么是拒绝服务攻击（DoS）与分布式拒绝服务攻击（DDoS）？  
两者有何不同？

它们的基本原理是什么？

黑客如何实现？

Q138 初级黑客如何快速、简单又有效地对目标服务器进行瘫痪攻击？

Q139 如何对拒绝服务攻击（DoS）与分布式拒绝服务攻击（DDoS）进行有效防护？

Q140 黑客如何判断与决定是否要清除进行入侵或破坏时留在服务器中的各种日志？

Q141 黑客入侵或破坏所可能在服务器中留下的各种日志要如何清理？

Q142 如何从各种日志中查看与找出可能的黑客入侵？

Q143 有哪些方法可以有效防止各种日志文件被黑客更改或删除？

附录 附录1 全球各地IP地址详细列表 附录2 端口列表 附录3 CurrPorts 附录4 NetStumbler 附录5 ProxyHunter 附录6 MultiProxy 附录7 Socks2HTTP 附录8 SocksCap 附录9 NetInfo 附录10 Angry IP Scanner 附录11 Mail Direct 附录12 NeoTrace Pro 附录13 VisualRoute 附录14 eMailTrackerPro 附录15 Startup 附录16 NetBrute Scanner 附录17 P Qwak 附录18 File Encryption Shell Extension 附录19 Brutus-AET2 附录20 Mailbag Assistant 附录21 SuperScan 附录22 X-Scan 附录23 各种软件密码破解工具 附录24 Advanced Instant Messengers Password Recovery 附录25 Magic Mail Monitor 附录26 EmEditor 附录27 wwwhack 附录28 流光（Fluxay） 附录29 N-Stealth 附录30 Shadow Security Scanner 附录31 SyGate Personal Firewall 附录32 TaskInfo 附录33 Net命令说明 附录34 at命令说明

<<黑客任务大作战>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>