

科海电脑技术丛书

黑客

就这么几招

阎 雪 编著

第2版

你害怕电脑被黑客入侵吗？

你清楚黑客如何进行攻击吗？

你知道如何避免被黑吗？

从黑客的历史、技术的演进、入侵的过程及防护，彻底剖析黑客的原貌

北京科海集团公司 出品

Hacker Technology

科海电脑技术丛书

黑客就这么几招

(第2版)

阎 雪 编著



你害怕电脑被黑客入侵吗？
你清楚黑客如何进行攻击吗？
你知道如何避免被黑吗？
从黑客的历史、技术的演进、入侵的过程及防护，彻底剖析黑客的原貌

北京科海集团公司 出品

内 容 简 介

本书从黑客攻击的角度出发,全面、详尽地介绍了黑客的种种攻击技术。书中对每种攻击方法都附有攻击实例,其中大部分攻击实例是从未公开过的;在介绍各种攻击方法的同时都给出了相应的用户对策,使广大网民和网络管理员可以保障自己系统与信息的安全,完善自己的网络环境。

本书的第1版在国内是畅销书,并且被台湾松岗电脑图书资料股份有限公司以繁体中文在台湾出版。自第1版畅销后,又有许多崭新的工具和技术出现,第2版在尽量保留第1版精华内容的基础上,加入了一些新的技术资料以及新近发生的重要黑客事件,并对本书所附光盘的相应软件作了更新。

本书适合计算机网络管理员、系统维护人员、网络用户、计算机爱好者以及大专院校有关专业的师生阅读参考。

注意: 光盘中的工具软件仅用于实验的目的,其宗旨是让您认识黑客,了解其攻击手段,从而防范黑客的非法攻击。若使用本光盘中的工具进行恶意破坏,必将受到社会的谴责和法律的制裁!

书 名: 黑客就这么几招(第2版)

作 者: 阎 雪

责任编辑: 张 律

出 品: 北京科海集团公司

印 刷 者: 北京市耀华印刷有限公司

发 行: 新华书店总店北京科技发行所

开 本: 787×960 1/16 印张: 38.125 字数: 601千字

版 次: 2002年3月第2版 2002年4月第2次印刷

印 数: 5001~8000

盘 号: ISBN 7-89998-022-4

定 价: 55.00 元(1CD)

第二版前言

随着因特网在中国的进一步发展,网络安全技术也显得越发重要了。在《黑客就这么几招》(2000年12月第1版)出版后一年的时间中,网络安全攻击以及防卫技术都有了显著的发展。例如,最近有一种被怀疑是国人编写的网络蠕虫病毒——"红色代码"在全球流行,被攻击的机器数以万计,这种病毒就使用了多种当今最先进的网络编程技术。

为了使广大网络用户以及网络管理员能够了解当今最新的网络攻击和防卫技术的发展情况,《黑客就这么几招》推出了第二版。在第二版中除了删除了第一版中基础知识介绍部分以外,尽量保留了上一版的精华内容,并加入了一些新的技术资料以及最近发生的重要黑客事件。

新增加的内容主要包括:第1章中的"2000年中美黑客大战纪实"、第5章"如何控制普通用户的计算机"、第6章中的"Windows下的溢出以及格式化串溢出"、第8章中的"X-Scanner介绍"、第14章"高级攻击技巧"以及第15章"攻击的善后工作"。

除了加入新内容外,还对书中介绍的一些软件进行了版本更新,使读者能够了解最新版本软件的新功能以及新特点。同时,本书附带的光盘中的相应软件均更新为最新的版本。

本书第二版在组织结构上仍然分4个部分,并对某些章节的顺序进行了调整,以便读者能够更好地理解其中的内容:

第1部分主要介绍黑客的历史、行为准则以及2000年中美黑客大战始末经过,包括第1章"黑客的历史"。

第2部分主要介绍黑客对普通用户的攻击手段,包括第2章"计算机病毒"、第3章"特洛伊木马"、第4章"网络炸弹"和第5章"如何控制普通用户的计算机"。

第3部分是本书的重点,主要介绍黑客对网站和网络的攻击手段。包括第6章"缓冲区溢出"、第7章"网络攻击的一般步骤及实例"、第8章"扫描器"、第9章"

密码破解"、第10章"sniffer"、第11章"利用Web进行攻击"、第12章"拒绝服务攻击"、第13章"欺骗攻击"、第14章"高级攻击技巧"、第15章"攻击的善后工作"和第16章"常见的系统漏洞及攻击实例"。

第4部分对网络安全防护体系的一些组成部分做了简要介绍,包括第17章"数据加密技术"、第18章"防火墙技术"和第19章"入侵检测系统"。

鉴于计算机技术的飞速发展,书中所述难免有不当之处,欢迎广大读者多提意见和建议,指出错误和不足。

编者

2001年11月

第一版前言

随着因特网的日益普及,上网对于许多人来说已经成为生活中必不可少的一部分,新老网民们通过网络来查找资料、交流信息。对于企业而言,网络更是占有举足轻重的地位,电子商务已经有逐步取代传统企业经营方式的趋势。但网络在带给我们极大便利的同时,也带来了另外一个棘手的问题,就是"黑客"问题。

由于因特网本身的设计缺陷及其开放性,使其极易受到黑客的攻击。根据美国有关安全部门统计,因特网上98%的计算机受到过黑客的攻击性分析,50%的机器被黑客成功入侵,而被入侵机器中有20%的管理员尚未发现自己已经被入侵。网络的安全性已经成为阻碍因特网在全球发展的重要因素之一。最近,美国包括"雅虎"、"亚马逊"、CNN在内的一些著名网站遭到黑客的大规模袭击,蒙受了巨大经济损失,引起了全世界对网络安全的密切关注。越来越多的人意识到,黑客已经成为全球新的公害,必须采取有力措施保护网络免受其扰。

在许多眼中,"黑客"是一些高深莫测的神秘人物,他们利用手中所掌握的技术肆意攻击网站、盗取商业机密。加上一些媒体对黑客事件不负责任的夸大报道,使得黑客以及黑客技术对大多数普通网民而言更多了一层神秘面纱。其实,黑客以及黑客技术并不神秘,也并不高深。一个普通网民在具备了一定基础知识之后,就可以成为一名黑客,甚至无须任何知识,只要学会使用一些黑客软件,同样可以对网络实施攻击,这也正是如今网络攻击如此盛行的原因之一。

俗话说,"知己知彼,百战不殆"。想要更好地保护自己不受黑客的伤害,就必须对黑客技术有一定的了解。只有对黑客的种种攻击手段有了详尽的认识,才能进行更有效、更具针对性的防护,使自己免受黑客攻击。我们本着使中国广大网民"认识黑客,了解黑客、防御黑客"的原则编写了这本书,从攻击技术的角度对黑客的种种手段作了详尽的介绍,目的在于让普通网民以及网络管理员对黑客技术有一个大致的了解,从而能够保护自己免受伤害,或把损失降低到最小程度。需要强调的是,黑客行为是违反我国有关法律规定的,如果对别人实施攻击并造成了损失,就必须对自己的

行为负法律责任。基于上述原因,本书在每介绍一种攻击手法的同时,都会给出与之相对应的详尽的防护方法,希望读者能够善用本书。

本书的重点在于介绍黑客的攻击手段和提供相应的保护措施,在组织结构上共分四个部分:

第1部分主要介绍黑客的历史、行为准则以及相关的基础知识,包括第1章“黑客的历史”和第2章“基础知识介绍”。

第2部分主要介绍黑客对普通用户的攻击手段,包括第3章“计算机病毒”、第4章“特洛伊木马”和第5章“网络炸弹”。

第3部分包括第6章“网络攻击的一般步骤及实例”、第7章“扫描器”、第8章“缓冲区溢出”、第9章“密码破解”、第10章“sniffer”、第11章“利用Web进行攻击”、第12章“拒绝服务攻击”、第13章“IP欺骗攻击”和第14章“常见的系统漏洞及攻击实例”。这一部分主要介绍黑客对网站、网络的攻击手段。

第4部分对网络安全防护体系的一些组成部分做了简要介绍,包括第15章“数据加密技术”、第16章“防火墙技术”和第17章“入侵检测系统”。

由于作者本人水平有限,加之时间仓促,书中难免有不当之处,还望广大读者多提宝贵意见。

编者

2000年11月

目 录

第1部分 基础知识

第1章 黑客的历史	2
1.1 黑客文化简史	3
1.1.1 古典黑客时代	3
1.1.2 现代黑客时代	6
1.2 黑客行为准则	7
1.3 黑客必须具备的技能	8
1.4 著名的黑客组织及黑客事件	9
1.4.1 大屠杀 2600	9
1.4.2 传奇黑客凯文·米特尼克	11
1.5 2001年5.1中美黑客大战纪实	14
1.5.1 起因	14
1.5.2 事态发展	16
1.5.3 对攻击所用技术的分析	17
1.5.4 对整个事件的反思	18

第2部分 攻击普通用户

第2章 计算机病毒	22
2.1 计算机病毒概述	23
2.1.1 什么是计算机病毒	23
2.1.2 计算机病毒的历史	23
2.1.3 计算机病毒的特征	25
2.2 计算机病毒的作用原理	27
2.2.1 计算机病毒的分类	27
2.2.2 病毒的作用机理	28
2.3 对猴子病毒的分析	28
2.3.1 猴子病毒的源代码分析	29
2.3.2 猴子病毒的杀毒要点	35
2.4 预防和清除计算机病毒	36
2.4.1 怎样预防计算机病毒	36
2.4.2 计算机病毒的检测与清除	39
2.5 宏病毒简介	42
2.5.1 什么是宏病毒	42
2.5.2 常见的宏病毒	43

2.5.3	宏病毒的预防与清除.....	44
2.5.4	宏病毒的编写.....	46
2.6	邮件病毒.....	49
2.6.1	邮件病毒简介.....	49
2.6.2	"爱虫"详解.....	49
第3章	特洛伊木马.....	62
3.1	特洛伊木马概述.....	63
3.1.1	特洛伊木马的概念.....	63
3.1.2	特洛伊木马的特点.....	63
3.1.3	未来木马的发展方向.....	64
3.1.4	木马的分类.....	65
3.2	常见的木马介绍.....	66
3.2.1	BO.....	66
3.2.2	国产木马冰河.....	74
3.2.3	预防和清除木马.....	77
3.3	木马的编写方法.....	82
3.3.1	隐藏进程技术.....	82
3.3.2	自动启动技术.....	83
3.3.3	远程监控技术.....	85
3.3.4	高级木马编程技术.....	92
第4章	网络炸弹.....	96
4.1	拒绝服务型炸弹.....	97
4.1.1	拒绝服务.....	97
4.1.2	OOB 攻击.....	97
4.1.3	IGMP 炸弹.....	98
4.1.4	特殊设备驱动器的路径炸弹.....	98
4.1.5	炸弹工具集 IP Hacker.....	99
4.2	电子邮件炸弹.....	100
4.2.1	什么是电子邮件炸弹.....	100
4.2.2	KaBoom! 邮件炸弹.....	101
4.2.3	防止邮件炸弹.....	102
4.3	OICQ 攻防.....	102
4.3.1	OICQ 简介.....	102
4.3.2	OICQ 的安全问题.....	103
4.3.3	OICQ 密码终结者.....	103

目 录

4.3.4	OICQSPY.....	104
4.3.5	OICQ 木马——GOP.....	109
4.3.6	其他 OICQ 黑客工具.....	113
4.4	在聊天室捣乱.....	117
4.4.1	聊天室穿墙术.....	117
4.4.2	聊天室炸弹.....	119
第5章 如何控制普通用户的计算机.....		120
5.1	对共享的攻击.....	121
5.1.1	什么是共享.....	121
5.1.2	对共享的一般攻击方法.....	121
5.1.3	利用共享密码校验漏洞.....	123
5.1.4	如何防止共享漏洞.....	124
5.2	对浏览器的攻击.....	124
5.2.1	什么是 MIME.....	124
5.2.2	MIME 头漏洞.....	125
5.2.3	MIME 头漏洞的解决办法.....	130
5.3	一次对 Windows 98 的攻击实例分析.....	130
 第 3 部分 攻击网络与网站		
第6章 缓冲区溢出.....		136
6.1	缓冲区溢出的基本原理.....	137
6.1.1	什么是缓冲区溢出.....	137
6.1.2	shellcode 的编写.....	143
6.2	通过 lpset 溢出获得 root 权限的实例.....	155
6.3	Windows 下的缓冲区溢出.....	159
6.3.1	返回地址的控制方法.....	159
6.3.2	Windows 系统下 Shellcode 的编写.....	161
6.3.3	Windows 下缓冲区溢出的实例.....	165
6.4	格式化串漏洞.....	169
6.4.1	格式化串漏洞原理.....	169
6.4.2	wu-ftpd 6.0 格式化串漏洞攻击实例.....	176
第7章 网络攻击的一般步骤及实例.....		181
7.1	攻击的准备阶段.....	182
7.1.1	攻击的步骤简述.....	182



7.1.2 确定攻击的目的.....	182
7.1.3 信息收集.....	183
7.2 攻击的实施阶段.....	185
7.2.1 获得权限.....	185
7.2.2 权限的扩大.....	186
7.3 攻击的善后工作.....	186
7.3.1 日志系统简介.....	186
7.3.2 隐藏踪迹.....	188
7.3.3 后门.....	189
7.4 一次攻击实例的详细过程.....	189
7.4.1 背景.....	189
7.4.2 攻击详细过程.....	190
7.4.3 从这次成功的攻击范例中得到的启示.....	200
第8章 扫描器.....	202
8.1 扫描器的相关知识.....	203
8.1.1 什么是扫描器.....	203
8.1.2 扫描器的分类.....	203
8.1.3 端口扫描原理.....	204
8.1.4 复杂的扫描技术.....	207
8.2 扫描器之王——nmap.....	209
8.2.1 简介.....	209
8.2.2 使用选项介绍.....	210
8.3 漏洞检查利器——Nessus.....	220
8.3.1 简介.....	220
8.3.2 Nessus的使用方法.....	220
8.3.3 对一次扫描结果的分析.....	223
8.4 大范围扫描工具——X-Scan.....	229
8.4.1 简介.....	229
8.4.2 所需文件.....	230
8.4.3 使用前的准备工作.....	231
8.4.4 使用方法.....	232
8.4.5 数据文件格式.....	234
8.4.6 插件接口.....	236

目 录

第9章 密码破解	242
9.1 选择安全的密码	243
9.1.1 什么是不安全的密码	243
9.1.2 什么样的密码才足够安全	244
9.2 Unix密码和John the Ripper	245
9.2.1 Unix密码的存放位置	245
9.2.2 John the Ripper用法详解	247
9.3 Windows 密码破解	256
9.3.1 Windows 密码导出工具 Pwdump	256
9.3.2 Windows 密码破解工具 L0phtCrack	258
9.4 远程密码破解工具——流光	260
9.4.1 主要功能	261
9.4.2 基本使用方法	262
9.4.3 对流光IV扫描结果的分析	275
9.4.4 流光IV使用实例	281
第10章 sniffer	284
10.1 sniffer 原理	285
10.1.1 网络技术与设备简介	285
10.1.2 网络监听原理	285
10.1.3 sniffer 的分类	287
10.1.4 网络监听的目的	287
10.1.5 一个简单的sniffer 程序	288
10.2 常见的免费 sniffer	290
10.2.1 sniffit	290
10.2.2 NetXRay	296
10.3 sniffer攻击实例	301
10.3.1 snoop简介	301
10.3.2 snoop 攻击实例	303
10.4 如何防御 sniffer 攻击	304
10.4.1 怎样发现sniffer	304
10.4.2 抵御 sniffer	304
10.4.3 防止 sniffer 的工具 AntiSniff	306
第11章 利用 Web 进行攻击	311
11.1 CGI的安全性	312
11.1.1 CGI为什么容易出问题	312

11.1.2	CGI 的问题出在哪里	312
11.2	ASP 的安全性	324
11.2.1	ASP 泄露源代码	324
11.2.2	ASP 编程时常常出现的问题	325
11.3	PHP 的安全性	326
11.3.1	PHP 程序存在问题的几个主要地方	326
11.3.2	如何增强 PHP 的安全性	335
11.4	常见的 CGI/ASP 漏洞	336
11.4.1	常见的 CGI 漏洞	336
11.4.2	常见的 ASP 以及 NT 相关漏洞	340
11.4.3	常见的 PHP 漏洞	343
11.5	CGI 扫描器——VoidEye	346
第12章	拒绝服务攻击	350
12.1	拒绝服务攻击概述	351
12.1.1	什么是拒绝服务	351
12.1.2	黑客为什么要使用拒绝服务攻击	351
12.1.3	拒绝服务攻击造成的后果	352
12.2	常见的拒绝服务攻击	352
12.2.1	Land	252
12.2.2	SYN flood	356
12.2.3	死亡之 Ping	360
12.3	最新的拒绝服务攻击方式——DDoS	361
12.3.1	DDoS 的原理	361
12.3.2	分布式拒绝服务攻击工具概述	362
12.3.3	TFN2000	363
12.3.4	预防分布式拒绝服务攻击	367
第13章	欺骗攻击	369
13.1	IP 欺骗攻击	370
13.1.1	信任关系	370
13.1.2	IP 欺骗的理论根据	371
13.1.3	IP 欺骗的全过程	372
13.1.4	米特尼克如何利用 IP 欺骗攻破 San Diego 计算中心	374
13.2	DNS 欺骗	382
13.2.1	DNS 的工作原理	382
13.2.2	DNS 欺骗的原理	384

目 录

13.2.3 DNS欺骗的实现过程.....	385
13.3 Web欺骗.....	387
13.3.1 什么是Web欺骗.....	387
13.3.2 为什么人们会受到Web欺骗.....	387
13.3.3 Web欺骗的工作原理.....	389
第14章 高级攻击技巧.....	393
14.1 渗透攻击.....	394
14.1.1 网络分析.....	394
14.1.2 进一步渗透.....	403
14.2 中间人攻击.....	404
14.2.1 概述.....	404
14.2.2 具体攻击方法.....	404
14.2.3 防范中间人攻击.....	408
14.3 对路由的攻击.....	408
14.3.1 查询路由器.....	408
14.3.2 破解路由器密码.....	409
14.3.3 路由协议的漏洞.....	410
第15章 攻击的善后工作.....	417
15.1 清除日志记录.....	418
15.1.1 Unix 日志的清除.....	418
15.1.2 Windows日志的清除.....	422
15.2 后门.....	424
15.2.1 简单后门.....	424
15.2.2 后门工具包——rootkit.....	427
15.2.3 内核级后门.....	430
第16章 常见的系统漏洞及攻击实例.....	438
16.1 各种服务存在的漏洞.....	439
16.1.1 FTP.....	439
16.1.2 SMTP.....	440
16.1.3 Named.....	440
16.1.4 Finger.....	444
16.1.5 HTTP.....	444
16.1.6 POP3.....	449
16.1.7 RPC.....	449

16.1.8	IMAP.....	454
16.1.9	SSH.....	454
16.1.10	Xinetd.....	457
16.2	操作系统的漏洞.....	458
16.2.1	AIX.....	458
16.2.2	FreeBSD.....	459
16.2.3	SCO.....	461
16.2.4	HPUX.....	462
16.2.5	SunOS.....	462
16.2.6	IRIX.....	464
16.2.7	Windows.....	465
16.3	利用sadminindex攻破日本政府某网站的实例.....	466

第4部分 网络安全防护

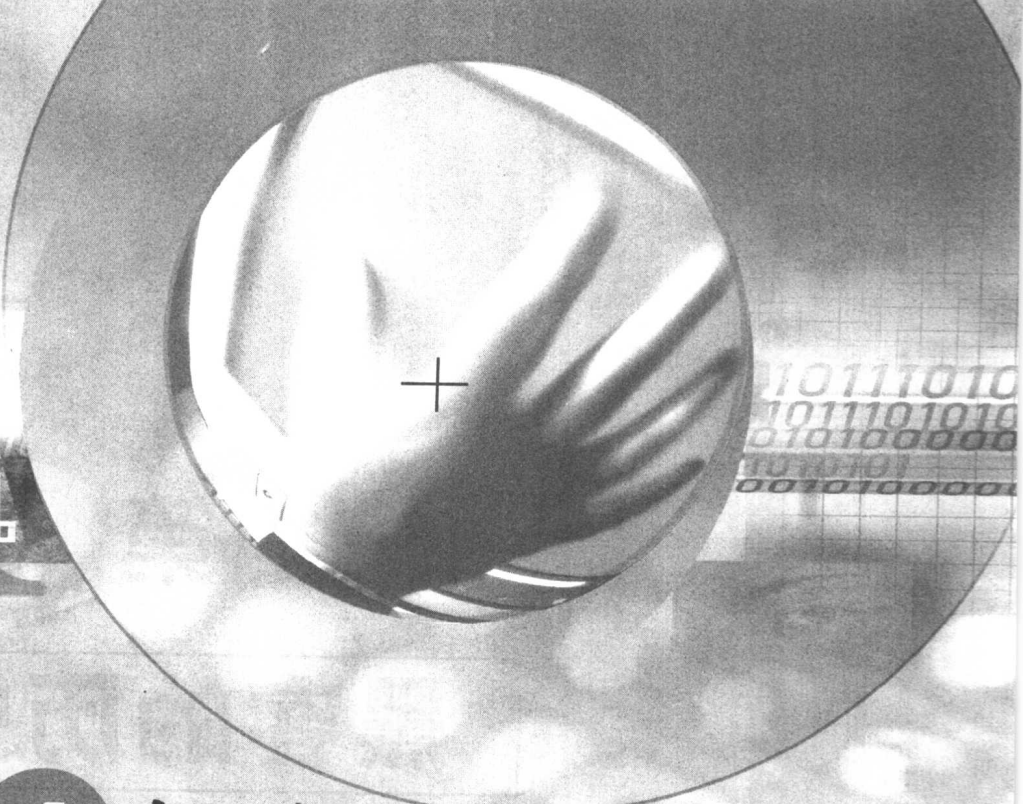
第17章 数据加密技术.....486

17.1	数据加密.....	487
17.1.1	概论.....	487
17.1.2	数据加密的实现方法.....	488
17.1.3	公钥加密算法RSA.....	490
17.2	邮件加密软件——PGP.....	493
17.2.1	PGP理论介绍.....	493
17.2.2	PGP FreeWare 6.5.3的使用方法.....	499
17.2.3	对PGP的攻击.....	508

第18章 防火墙技术.....515

18.1	防火墙基础.....	516
18.1.1	防火墙的概念.....	516
18.1.2	构造防火墙.....	516
18.1.3	防火墙的作用.....	517
18.2	防火墙的分类.....	518
18.2.1	包过滤防火墙.....	518
18.2.2	应用级网关.....	521
18.2.3	状态监测防火墙.....	523
18.3	FireWall-1防火墙简介.....	524
18.3.1	主要功能介绍.....	524

18.3.2	访问控制设置	529
18.4	天网个人防火墙简介	531
18.4.1	安装方法	531
18.4.2	天网个人版防火墙运行与设置	532
18.5	攻击防火墙	543
18.5.1	对防火墙的扫描	543
18.5.2	通过防火墙留后门	546
18.5.3	已知的防火墙漏洞	547
第19章	入侵检测系统	553
19.1	IDS概述	554
19.1.1	入侵检测系统的分类	554
19.1.2	遭受攻击时的迹象	555
19.2	利用系统日志做入侵检测	556
19.2.1	重要的日志文件	556
19.2.2	利用系统命令检测入侵动作	559
19.2.3	日志审核	561
19.2.4	发现系统已经被入侵之后	563
19.3	常见的入侵检测工具介绍	565
19.3.1	Watcher	565
19.3.2	日志审核工具Swatch	567
19.3.3	访问控制工具Tcp wrapper	569
 附 录 		
附表1	木马程序	577
附表2	OICQ工具	579
附表3	炸弹软件	581
附表4	扫描工具	583
附表5	sniffer	585
附表6	解密工具	586
附表7	安全防御	589
附表8	其他工具	592



第 1 部分

基础知识

- 黑客的历史