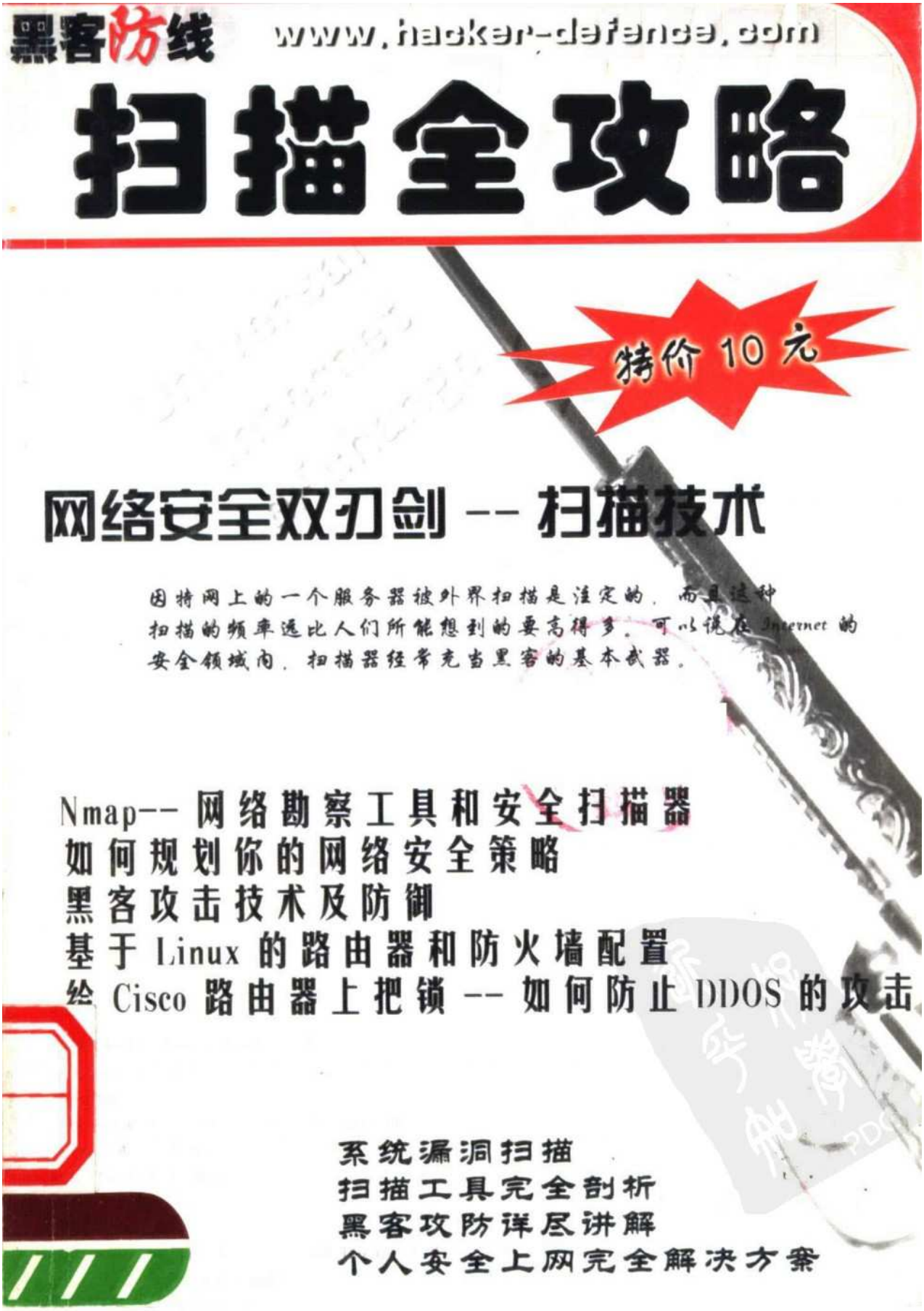

ISBN 7-900070-45-1/TM.13
9 787900 070456
北京地海森波网络技术有限公司制作
万方数据电子出版社出版
软件渠道总经销：北京正普公司
电话：010-82671133

成长之路

瞬息万变的网络时代，网络安全问题越发显得重要，我们投身于网络安全事业的研究，相继推出《黑客防线秘笈》，《黑客防线》第2、3、4、5期系列产品，从黑客角度介绍网络安全知识，帮助企业、家庭、个人用户构造安全的上网方案，提高广大读者的网络安全（防御）意识。现在，我们的产品已经深受读者群体的喜爱，为了能够更好的服务于读者，我们联合业界网络安全专家，对《黑客防线》全面改版，使她成为国内惟一的介绍网络与计算机安全的电子期刊，伴随读者在21世纪这个互联网时代共同发展，共同成长。

第5期作为过渡型产品，仍采用160版面，但内容上已经做出栏目规划。从第6期我们在保质保量前提下，将版面改为128版，而实际容量仍保持10－12万字不变，定价由19.8元做下 调，并将联合一些从事网络安全研究的行业人士，提高稿源质量，使得读者买的称心，看的如意。

在这期我们采用专栏的形式，涉及到黑客攻击、网络安全的方方面面，内容更全、更新、更实用。在这里，你可以实时了解黑客动态；掌握黑客基础知识；洞察黑客的攻防技巧；聚焦网络的安全漏洞；完全的网络安全解决方案；彻底的黑客工具实例解析。想你之所想，给你之所需，既把握最新变化，又贴近实际应用。重点部分定位在网络扫描工具的剖析和实际应用上，这在网络安全日益紧迫的今天，网络扫描成为最急需解决的首要问题，它不仅成为黑客成功入侵的关键步骤，也是网络管理人员的得力法宝，在入侵、反入侵这场战争中，扫描器一直扮演着这种亦正亦邪的角色。

当然，我们还有很多不足之处需要您来指点，欢迎您来信提出宝贵的意见；欢迎您来稿写出您的心得，让我们读者共同分享你得成功。

由于《黑客防线》系列产品的相继推出，现在盗版市场已经出现了我们刊物的配套光盘，如您已经购买此类光盘，请寄至我们公司，我们将免费赠予正版。

请记住我们的地址：北京市中关村邮局 008 信箱

北京地海森波网络技术公司技术部收

邮政编码：100080

目 录

黑客动态

黑客案例

基础知识

· Pc friend ·

制　　作：北京地海森波网络技术公司
出　　版：万方数据电子出版社出版
ISBN7－900070－45－1/TM. 13
通信地址：北京市中关村邮局 008 信箱
邮　　编：100080
技术支持电话：（010）82672099
E－mail：Pcfriend@ mail. 263. net. cn
Pcworld@ public. gb. com. cn
wzh417@ 263. net
编　　辑：郭聪辉　刘东亚
彭荣全　王晓东
制　　作：王进才　施剑峰　袁刚
美术设计：宋成林　温洋　王凤　王晴
发行部电话：（010）62141360
发行部传真：（010）62141446
定　　价：28.00 元（光盘＋手册）

光盘内容检索

特别推荐

软件名称： Fantast15
软件说明：程序用来得到密码信息，并发送到指定邮箱。可以用来得到拨号上网的密码电话号码、Oicq 密码等。本站收集上一版本为 1.4（注：1.5 版与 1.4 版启动程式不一样），自启动程序 c：\windows\`.exe，把 system.ini 中[boot]下的 shell = Explorer.exe `.exe 改成 shell = Explorer.exe
光盘路径： \tuijian\fantast\fantast15.zip

软件名称：Zz_op
软件说明：“蜘蛛 OicqPass beta 1”（需要 VB6 运行库）运行后即可记录所有 Oicq 登陆号和密码。软件可任意改名，建议放在 Windows 的 System 目录下，记录密码文件是同目录下和更改名一样的 INI 文件，软件支持最新的 Oicq2000b 0106 版本
光盘路径： \tuijian\zz_op\zz_op.zip

软件名称：OicqPatch0106
软件说明：Oicq2000 的补丁程序，该补丁可以对 Oicq2000/0106 版本有几个方面的改动：
1. 可以更改 Oicq 客户端的默认端口，由原来的 4000 改为你自己定义的端口号。
2. 可以更改 Oicq 程序默认的浏览器，由原来的腾讯浏览器改为微软浏览器。
3. 可以去掉 Oicq 发送消息和接收消息窗口中的广告。
光盘路径： \tuijian\Patch0106\OicqPatch0106.zip

· Pc friend ·

软件名称：Ld2000_7x_key
软件说明：Lockdown2000 最新的版本的注册机，这可是本刊黑编们精心为大家准备的好东东哦 ：)
光盘路径：\tuijian \lockdown \ld2000_7x_key. zip

软件名称：Cr_pcguard
软件说明：中国墙（个人电脑版）V1. 0 破解文件，下载原版后安装，将破解文件的 ZIP 包释放到安装目录，覆盖原来的 EXE 或 DLL 文件，如果 ZIP 包里有“注册文件 . REG”文件，请先双击它，将注册信息添加到注册表里，这样一般就可以完成注册了！如果还提示没有注册，请输入任意注册码后重新运行！
光盘路径：\tuijian \cr_pcguard \cr_pcguard. zip

软件名称：Twsetup203
软件说明：2001 年 1 月 17 日推出的，天网防火墙个人 V2. 03 版，适用于 Windows 2000/NT(sp6)/98/ME. 已经兼容 WindowsME/NT(sp6)/98/ME 已经兼容 WindowsME/NT。
光盘路径：\tuijian \twsetup203 \twsetup203. exe

软件名称：school55
软件说明：四海网络教室 V1. 55，无须注册即可同时管理多达 70 台计算机。电子举手、电子教鞭、远程启动、网络通知、屏幕监看、屏幕广播、遥控辅导、示范教学……完全隐藏学生程序（绿色软件）。
光盘路径：\tuijian \school \school55. zip

软件名称：zonalarm
软件说明：功能相当强大、全面的个人版防火墙，可以随时查看本地所有的对 Internet 的连接，并可以允许连接或强制断开，防木马必备工具。
光盘路径：\tuijian \zonalarm \zonalarm. exe

软件名称：Nettools1129
软件说明：Net Tools(Build 1. 2. 2000. 0526)
1. 本地信息：Windows 版本，Winsock 版本，IP 地址，网卡地址；

2. 网络连接监视：列出所有 TCP、UDP 连接、远端地址和端口；
3. POP3，SMTP：可以发送和接收带附件的邮件；
4. 统计信息：IP、TCP、ICMP、UDP 数据的统计信息；
5. 路由跟踪；
6. IP 地址和域名地址的互相转换。

光盘路径： \tuijian \nettools1129 \nettools1129. zip

软件名称：7473_way
软件说明：Way 远程控制系统 2.0(网络注册表杀手)版，该版本修正了 1.0 的许多 Bug，新增了许多功能，如窗口控制，系统颜色更改，点对点聊天通讯，拨号控制，光驱控制，剪切板监视等。
光盘路径： \tuijian \way \7473_way. zip

软件名称：Iparmor306
软件说明：木马克星 3.06 版，采用动态监视网络连接和静态特征字扫描技术，可以查杀 3794 种国际木马，79 种电子邮件木马；可查杀冰河所有版本以及黑洞所有版本，支持在线升级。
光盘路径： \tuijian \iparmor306 \iparmor306. zip

软件名称：Eporterdemo
软件说明：Eporter 是一个网络监理工具，它具有 UDP or ICP Packet Port Forwarding 及网路即时监控管理的功能，可以通过中间电脑隐藏上站 IP，而且还有不错的连线数管理功能。
光盘路径： \tuijian \eporter \eporterdemo. zip

软件名称：冰河 3.3
软件说明：又一个修改后的冰河程序，称为冰河 3.3 版本，据说没有通用密码，本刊编辑部特别推荐
光盘路径： \tuijian \binghe \binghe33. zip

软件名称：Oicq2kpass
软件说明：Oicq2000 的密码破解工具(非自动登陆无法显示其号码)，压缩包

内含源程序。
光盘路径：\tuijian \oicq2k \oicq2kpass. zip

软件名称：Gop12
软件说明：GOP 1. 2(Get Oicq Password)版，Oicq 密码窃取木马，主要功能：定义目录、运行后删除源文件、服务文件名、钩子文件名、定义注册表键名、当记录数超过 XX 个时开始清理、邮件发送服务器、检查间隔、邮件优先级、发送测试、使用欺骗窗口、测试、按钮类型、图标、窗口标题、欺骗信息、文件绑定、宿主文件、文件图标、捆绑。
光盘路径：\tuijian \gop12 \gop12. zip

软件名称：LeakTest
软件说明：Leak Test 可以测试你的防火墙有用，是否可以抵抗任何形式的入侵。LeakTest 的原理如下：程序会尝试建立一个标准的 TCP 连接到原创公司(GRC. com)主机的 FTP 的端口 21 ，如果连接成功并确定取得传送资料的权限后，LEAK TEST 会马上断线，并告诉你，你的防火墙无法阻挡这次渗透，木马、广告间谍等能穿过你的防火墙。
光盘路径：\tuijian \LeakTest \LeakTest. exe

软件名称：Compreg
软件说明：注册表文件比较 2. 0 版，
功能：详细比较同一台运行 Win9X 的计算机上的两份注册表文件；速度：从载入文件到比较完毕，仅需几秒钟；用途：监视注册表的变化、防黑、破解软件的使用次数和天数(如果你有灵性和耐心)。
光盘路径：\tuijian \zhuce \comreg. zip

软件名称：FolkOicq0106
软件说明：2001 年 1 月 6 日最新版的 Oicq，这东西肯定是越新越好了 :)
光盘路径：\tuijian \Qip \FolkOicq0106. zip

软件名称：dll 文件
软件说明：如果你的一些软件运行的时候缺少链接文件，可以到这个目录下找

找，相信对你会有所帮助
光盘路径：\tuijian\dll*.*

软件名称：HDPRT
软件说明：修复由于误操作或病毒发作引起的硬盘数据丢 失。如果你用一些杀毒软件的修复硬盘功能和 NDD 没有效果，那么你可以试试它。下载后运行 README. EXE，有详细说明。
光盘路径：\tuijian\hdprt\hdprt. zip

安全防御

软件名称：Nn29
软件说明：可有效防御 Winnuke 和 OOB 的攻击。强烈推荐！
光盘路径：\anquan\nn29. zip

软件名称：WebWatch
软件说明：WebWatch 可以检测到个人主页的变化情况，哪怕是微小的变化。只要将站点添加到 WebWatch，然后点击 Run 就可以了。
光盘路径：\anquan\Web1106WatchV1. exe

软件名称：X - NetStat 3.0
软件说明：X - NetStat 3.0 运行在 Windows 9X/NT 上，监视当前网络和互联网络连接。XNS 可显示每一个当前连接的本地/远程网络地址（主机名或 IP）、本地/远程端口和连接状态，支持 ICMP、UDP、TCP 协议。
光盘路径：\anquan\XNS3SETUP. EXE

软件名称：Yoko130
软件说明：这个工具在用户名单的基础上使用 FTP 多线程的暴力解法来寻找愚蠢用户，管理员如果用这个软件发现了密码，应该立即为其更改密码。这个软件也可以利用指定的密码或者利用用户名 + 字符串的方法，进行攻击。
光盘路径：\anquan\yoko130. zip

· Pc friend ·

软件名称：Findhost
软件说明：根据给定的地址和端口号查找机器。1.1 版新增多线程同时搜索技术，可以将搜索速度提高 10 倍以上。用它查找中了 NetSpy 的机器很好用。
光盘路径：\anquan\IPFA－1.1.0.TAR.GZ

软件名称：Nemesis11
软件说明：你是不是老担心自己的机器是否有木马啊？这是帮你检查的工具，能查出上百种木马呢，最大的好处是能帮你的朋友远程扫描。
光盘路径：\anquan\nemesis11.zip

软件名称：Real Time Cookie Cleaner
软件说明：由于现在的浏览器大多支持 Cookie 的功能，所以让你在上网的时候更加方便了，不过，相对也增加了不少危险性。这个软件可以帮你立即将电脑中的 Cookie 给清干净，让你在上网的时候更加安全。除此之外，还可以将你上过的网站记录以及最近所打开的一些文件一次清干净。
光盘路径：\anquan\rtcc15.zip

软件名称：IP 守护天使
软件说明：只要有人扫描你，它就会立即弹出窗口，并告诉你此人的 IP，然后怎么办。自己看着办吧！而且有可能对方还会掉线哦 :)
光盘路径：\anquan\nfrbof.exe

软件名称：Ailcut
软件说明：中文砍信机，如果有人给你发邮件炸弹就用得上了。当你打开邮箱收信时运行它，先看看有哪些信可以收、哪些不收，并可以直接远程在服务器上把它删除。
光盘路径：\anquan\ailcut.zip

软件名称：Lockdown2000cn
软件说明：Lockdown2000 的汉化程序。
光盘路径：\anquan\lockdown2000cn.exe

软件名称：WinZapper
软件说明：该工具编辑在 Windows NT 4.0 和 Windows 2000 中的安全事件日志。就我们所知，WinZapper 是第一个在安全日志中删除一行而不是删除全部日志的工具。可在 Windows 运行后实现。
光盘路径：\anquan\WinZapper.zip

软件名称：Weedlog
软件说明：weedlog 是一个日志包，在没有路由器的系统中完成网络连接的功能。它目前支持 ICMP、IGMP、TCP 和 UDP 协议，支持输出到标准输出设备的文件或系统日志。
光盘路径：\anquan\WEEDLOG－1.0.0.TAR.gz

软件名称：网络卫兵
软件说明：网络卫兵完全解密版，彻底解除了试用版的限制
光盘路径：\anquan\webws.zip

软件名称：Tripwall 0.10a
软件说明：这是 Colin Lee 写的一个文件完整性检查工具和入侵检测系统。Tripwall 是用来重新启动系统或某一文件被改变后刷新 ram 驱动的，/bin/login, /bin/ls, /bin/ps, 或/bin/sh，对其进行刷新的工具。
光盘路径：\anquan\TRIPWALL.TAR.gz

软件名称：WinDog Deception Toolkit
软件说明：该工具包是基于伪造邮件收发守护进程的两个 perl 程序，用来完成基本的入侵检测。它分别发送邮件和远程登录邮件服务器。要使用该工具包，你的系统必须安装有 Win32 Perl。
光盘路径：\anquan\WINDOG－DTK.zip

软件名称：Zonalm20
软件说明：一个不错的防火墙软件，它可以检查你计算机上与因特网所有的连接，并控制哪个程序可以进行因特网的存取，可报出于你联结的 IP，还可看出是什么程序。
光盘路径：\anquan\zonalm20.exe

· Pc friend ·

软件名称:Anony Cookie
软件说明:能隐藏你上网的电话、IP、帐号,你只要在上网前运行它就 OK 了。
光盘路径:\anquan\setupac_b2.zip

软件名称:The Cleaner 3.0
软件说明:MooSoft Development 写的 Cleaner 是一个用于 Windows 95/98/NT/2000 的 Trojan 的扫描引擎,并清除系统已经有的病毒。Cleaner 使用原始的方法独特地鉴别文件,它能够发现 Trojans,即使这些 Trojans 已经改变了它们的文件名或是文件的大小,或是附加到其他的文件上去了
光盘路径:\anquan\cleaner31024.exe

软件名称:IPHacker
软件说明:可以有效地检测 Win95/WinNT 的 OOB 漏洞和 Win95/Win98 的 IGMP 漏洞,可以使你的计算机出现蓝屏/Modem 掉线/重启的现象。
光盘路径:\anquan\iphackerv.exe

软件名称:Attacker 2.1
软件说明:它是一个简单的 TCP 端口监听工具,监听一系列的端口,当端口有链接请求时会发出声音警报通知你。该程序作为一个看门狗及时通知你有人试图通过 Internet 探测你的计算机。
光盘路径:\anquan\Attacker.zip

软件名称:ZoneAlarm
软件说明:ZoneAlarm 可以保护你的电脑,防止 Trojan(特洛伊木马)程序,Trojan 也是一种极为可怕的程序。ZoneAlarm 可以帮你执行这项重大任务,而且还是免费的。
光盘路径:\anquan\zonalarm1019.exe

软件名称:Trojan Remover
软件说明:一个专门用来清除特洛伊木马和自动修复系统文件的工具。能够检查系统登录文件、扫描 WIN.INI、SYSTEM.INI 和系统登录文件,且扫描完成后会产生 Log 信息文件,并帮你自动清除特洛伊木马和修复系统文件。
光盘路径:\anquan\Trjsetup1031.exe

软件名称:Tocsin
软件说明:Tocsin 是一个基本的入侵检测系统,使用包过滤对来自可疑服务器的可能的攻击并进行防范。
光盘路径: \anquan \Tocsin. zip

软件名称:Languard
软件说明:Languard 类似于 eEye 的 iri100,有网络监视器、检测口令嗅探器、网络存取控制、以太网监控、连接状况、限制过滤地址、截获以太网内数据、监听所有输出输入的 TCP/IP 数据包、安全级别的设置等功能,是个相当不错的安全工具。2000 下测试完成。
光盘路径: \anquan \languard. zip

软件名称:Anomy Sanitizer 1. 25
软件说明:Anomy Mail Sanitizer 是 Bjarni R. Einarsson 写的一种过滤器,它是用来阻止基于电子邮件的攻击(比如像特洛伊和病毒)的传播。它读一个 RFC822 或 MIME 信息,删除或是重新命名附件,限制一个 MIME 头文件的长度或是通过使 JavaScript 和 Java 无效,来清理一个 HTML 文件。它使用单一的纯 PERL MIMIDE 分析,使它的分析比其他同类产品更有效,更精确。它还支持对第三方病毒的扫描。
光盘路径: \anquan \ANOMY - SANITIZER - 1. 20. TAR. gz

软件名称:Ostronet 5
软件说明:OstroSoft 互联网工具是一套完整的网络信息工 具。它提供给你如下重要的信息: 在域中哪些计算机在运行特殊服务,例如,在域中有多少新闻服务器是可接受访问的(域扫描器);在计算机上正在运行什么网络服务(远程还是本地),例如: WEB 服务器, Telnet, 邮件服务器, FTP, Finger 等等(端口扫描器); 允许你测试远端主机是否在运行,是否容易接近你的系统,到远端主机所花的时间(Ping); 显示从本机到远端主机的 TCP 包的路径(跟踪路由); 显示在本机上有效连接(Netstat), 把主机名解析成 IP 地址和逆向解析(主机解析器 - dns); 对特定网络(网络信息)返回相关信息(地址、电话、传真、管理员姓名、DNS 服务器); 显示关于你的计算机(本机信息)的网络延迟信息(IP

地址、主机名、Winsock 版本等)；能帮助你在网络中找到隐藏的资源。
光盘路径： \anquan \ostronet5. 2Build40927. zip

软件名称：MausTrap
软件说明：Edwill Leighton 写的 MausTrap 是一个小型但很有效的安全程序，它可以阻止没有口令的用户登录 Windows 系统。它会使一些 Windows 的热键无效，比如 Alt + Ctrl + Del, Alt + Tab 等。它还能隐藏工具栏和 Windows 桌面，使你无法使用 Windows 系统直到你提供了正确的口令。如果你不想你的计算机空闲的时候被其他人使用，那就安装 MausTrap 吧。网吧安全特别适合。
光盘路径： \anquan \MausTrap. zip

软件名称：Anomy – sanitizer – 1. 20
软件说明：该过滤器将重写邮件/模仿文件头以试图减慢基于电子邮件的 Virii 和 Trojans 的传播。附件文件将被重写以便使它们不会再被看起来是可以执行的，文件头长度将被限制到合适长度以避免缓冲器溢出，使用外部的防病毒扫描器对附件进行扫描，或者只从邮件中删除附件成为可能。
光盘路径： \anquan \ANOMY – SANITIZER – 1. 20. TAR. gz

软件名称：Adore – 0. 14
软件说明：虽然 Adore 的使用已经非常广泛了，但仍有些问题需要注意：对于安装了 adore 的人都必须选择自己的 ELITE – CMD 才能防止被扫描，HIDDEN – PORT 也应该改 变。当提到 MODVERSIONS 转换时，Adore 将被作为 MODVERSIONS 的内核来编辑。MODVERSIONS 的内核看起来像一个/proc/ksyms 文件。
光盘路径： \anquan \ADORE – 0. 14. TAR. gz

软件名称：IRIS100
软件说明：eEye 公司的另一个“安全”作品 IRIS100，可以检测网络状态和监视入侵、嗅探，是一个绝对好的捕获、解码和扫描的工具(可以在得知有被入侵的时候告知你，不过就是那该死的警报声听得人顶不顺耳)IRIS100 不像其他网络嗅探器，它有高级、完整的技术组合，更好地让你了解到网络的状态。
光盘路径： \anquan \IRIS100 . exe