

黑客



工具·进阶篇

仲治国 白海峰 编著

全解∞种兵器析

致命
絕殺

揭秘∞种
常用兵器
黑客攻防
完全精通



精彩光盘

- 杀毒防黑软件
- 杀毒防黑攻略教程
- 黑客攻防电子书
- 黑客绚丽屏保

黑暗中的慧眼
查看电脑安全隐患
步步为营
进程与端口的攻防实战
控制与反控制
互联网远程入侵与防御
突破封锁
无线路由器的账号密码破解
揭露隐形的秘密
曝光加壳、脱壳实战操作
穿越毒笼
流行病毒查杀方法
无形的黑手
无线网络安全攻略

黑 凌

全 解 析 工 具 进 阶 篇

仲治国 白海峰 编著

致命
絕殺



电脑报电子音像出版社
CPCW ELECTRONIC & AUDIOVISUAL PRESS

内容提要

本手册专为黑客攻防与网络安全爱好者量身定制，以实例演练形式，借助不同黑客攻防软件，为读者详细剖析黑客攻防手段，并提供相应防护措施。手册内容共计10章，内容涵盖扫描嗅探欺骗、进程与端口攻防、直面网络盗号、加密解密、病毒问题处理、木马植入与远程控制、网吧攻防、网站攻防、漏洞攻防以及服务器攻防。丰富的案例、详尽的操作步骤将给读者提供最快捷的帮助，迅速掌握黑客与网络安全技术。

光盘要目

- 《可牛杀毒软件》（电脑报专用版）
- 杀毒防黑软件
- 杀毒防黑攻略教程
- 黑客攻防电子书
- 黑客绚丽屏保

版权所有 盗版必究

未经许可 不得以任何形式和手段复制和抄袭

声明：使用网络技术攻击他人计算机属于违法行为，读者切勿用本手册内容对他人计算机进行恶意攻击，否则后果自负！

黑客88种兵器全解析

编 者：仲冶国 白海峰

责任编辑：连 果

版式设计：杨 亚

出版单位：电脑报电子音像出版社

地 址：重庆市双钢路3号科协大厦

邮政编码：400013

服务电话：(023)63658888-12031

发 行：重庆电脑报经营有限责任公司

经 销：各地新华书店、报刊亭

C D 生 产：四川省釜山数码科技有限公司

文本印刷：重庆市联谊印务有限公司

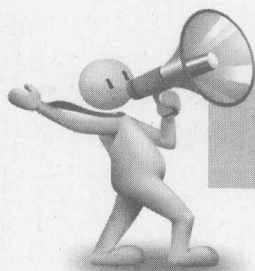
开本规格：787mm×1092mm 1/16 17印张 200千字

版 号：ISBN 978-7-89476-480-5

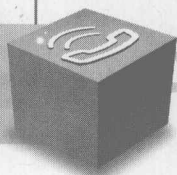
版 次：2010年10月第1版 2010年10月第1次印刷

定 价：35.00元(1CD+手册)

前言



揭秘黑客谋略与兵器精髓



这是一套全面指导黑客入门与实战的黑客图书

这是一套深刻解析攻防工具及应用的黑客图书

这是一套完全精通攻防谋略与技巧案例的黑客图书

网络就是战场、安全就是用兵。

战场上硝烟弥漫，鲜血迸溅；网络中针锋相对，明争暗斗！

黑客世界的刀光剑影总让人感到神秘莫测。

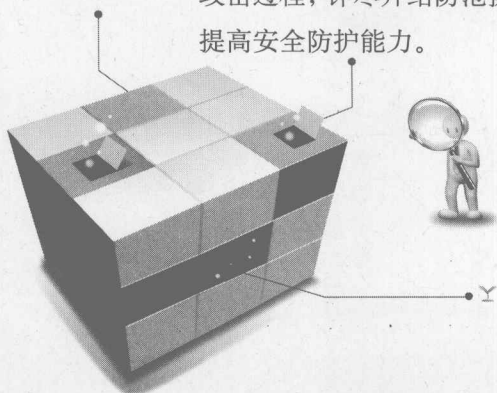
正所谓兵来将挡，水来土掩。只要我们抱着“勿恃敌之不来，恃吾有以待之”的精神，必能将各种危机化解于无形！熟读兵书三百遍，不会用兵也能防。

一名技艺高超的黑客无非体现在以下三方面：其一是掌握常见的黑客攻防手法，其二是娴熟的黑客工具应用，其三是独到的谋略技巧施展。本系列图书正是围绕以上三方面的黑客攻防必备技能为读者全面展开并详细解读。

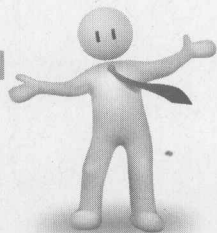
《黑客入门与成长秘技 108 招》：通过 108 招攻防技巧，由浅入深地为大家讲解了黑客成长必备的技能，让大家快速步入黑客之门。

《黑客 88 种兵器全解析》：精选了黑客最常用的 88 种攻防工具，通过工具的实战操作帮助读者快速领悟黑客攻防手段。

《黑客攻防 36 计》：剖析了与黑客斗智斗勇的 36 个实战案例，全面解析黑客攻击过程，详尽介绍防范操作步骤，帮助你快速掌握黑客攻防的深度谋略与技巧，提高安全防护能力。



编者
2010 年 9 月



光盘精彩导航

实用功能

本光盘可自启动电脑，并进入 Windows PE 系统，进行系统维护、杀毒等。还可通过 Ghost 软件进行系统一键备份，系统还原等操作。该光盘功能完善、实用，是你维护电脑的随身宝典。

正版软件超值赠送
可牛免费杀毒电脑报专用版

全解析 ∞种兵器 黑客

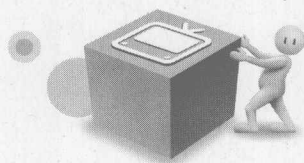
可牛杀毒软件
杀毒防黑软件
杀毒防黑攻略教程
黑客攻防电子书
黑客绚丽屏保

杀毒防黑软件

恶意插件清理工具
 加密解密工具
 浏览安全工具
 漏洞检测修复工具
 杀毒反黑工具
 数据恢复工具
 网吧管理工具
 系统安全辅助工具
 系统监视工具
 账号保护工具
 远程控制工具

杀毒防黑攻略教程

2008 灰鸽子超级简单免杀
 个人电脑的安全设置
 揭示局域网抓鸡过程
 揭示另类木马躲避杀毒软件过程
 清除被感染系统中的病毒代码

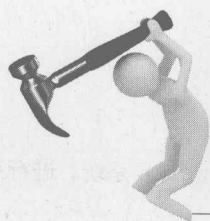


黑客绚丽屏保

AutoAssault_SS_setup
 Cossacks2_Screensaver1
 MatrixWorld 3D Screensaver
 Terminator3
 黑客帝国3D屏保
 开屏桌面屏保系统
 空中战争屏保
 蓝天银鹰屏保
 联想电脑重启屏保
 坦克屏保
 武装直升机屏保
 子弹屏保

黑客攻防电子书

第1章 扫描嗅探与欺骗
 第2章 进程与端口攻防
 第3章 直面网络盗号
 第4章 加密、解密与突破
 第5章 穿越毒龙

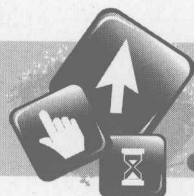


目录

CONTENTS

致命绝杀

黑客88种兵器全解析



第1章 扫描、嗅探与欺骗

X-scan查看电脑隐患应用实例001

- 一、X-scan简介.....001
- 二、X-scan的基本使用.....001
- 三、高级设置.....002

国产第一扫描器“流光”.....004

- 一、流光简介.....004
- 二、批量主机扫描.....005
- 三、指定漏洞扫描.....007

局域网安全扫描专家LANNSS008

- 一、LANguard功能简介.....008
- 二、应用实战.....008

扫描操作系统信息.....010

- 一、X-scan探测系统信息.....010
- 二、Ping命令也能探测系统信息.....011
- 三、借助网站获取操作系统信息.....012

用ProtectX防御扫描器追踪013

- 一、ProtectX帮你忙.....013
- 二、防护扫描器攻击的要点.....014

经典嗅探器Iris014

- 一、嗅探器的工作原理.....014
- 二、实例介绍Iris.....015

三、怎样防御嗅探器.....017

经典嗅探器之NetXray017

- 一、NetXray简介.....017
- 二、应用实战.....018
- 三、重要功能说明.....019

打造傻瓜化的蜜罐——KFSensor019

- 一、KFSensor简介.....020
- 二、蜜罐设置.....020
- 三、蜜罐诱捕.....020

邮箱账户欺骗与防范.....021

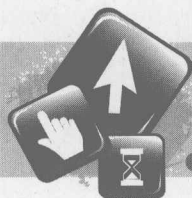
- 一、邮箱账户伪造揭秘.....021
- 二、隐藏邮箱账户.....021
- 三、垃圾邮件的防范.....022
- 四、重要邮箱的防范之道.....024
- 五、查找伪造邮箱账户的发件人.....025

Administrator账户的删除与伪造025

- 一、更改账户名.....025
- 二、伪造陷阱账户.....027

识破混迹管理员组的Guest账户029

- 一、虚假的管理员账户是这样炼成的.....029
- 二、如何识破Guest账户.....029
- 三、Guest账户的安全管理.....030



第2章 进程与端口攻防

当心病毒寄生SVCHOST.EXE进程032

- 一、认识SVCHOST.EXE 032
- 二、识别SVCHOST.EXE进程中的病毒 032

判断Explorer.exe进程真假033

- 一、什么是Explorer.exe进程 033
- 二、Explorer.exe容易被冒充 034

巧用Windows进程管理器035

- 一、进程管理 035
- 二、恶意进程分析 035

超级巡警保护系统进程036

- 一、全面查杀 036
- 二、实时防护 036
- 三、保险箱 036
- 四、系统安全增强工具 037
- 五、妙用SSDT工具清除流氓软件 038

专业的进程管理工具——AutoRuns038

- 一、启动项管理 038
- 二、进程实战解析 039

进程管理的好帮手Process Explorer 040

- 一、进程管理 040
- 二、进程加速 043

3389端口入侵与防范043

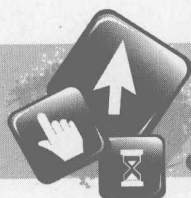
- 一、什么是3389端口 043
- 二、3389入侵实例剖析 044
- 三、3389端口安全防范 044

扫描端口确保电脑安全045

- 一、用SuperScan扫描端口安全 045
- 二、用NetBrute Scanner扫描端口 045

玩转NC监控与扫描功能046

- 一、监听本地计算机端口数据 046
- 二、监听远程计算机端口信息 047
- 三、将NC作为扫描器使用 047



第3章 直面网络盗号

阿里旺旺“明文”密码漏洞实测048

- 一、旺旺进程中“明文”保存密码账号 048
- 二、旺旺中登录邮箱也“明文”显示 049
- 三、虚假钓鱼网站“盗”旺旺密码 049

当心QQ被盗——“爱Q大盗”050

- 一、配置QQ木马 050

- 二、突破软件的限制 050
- 三、运行木马 051

手机QQ不用密码也能登录051

在线盗号的“QQ终结者”052

- 一、配置盗号木马 052
- 二、上传文件、收获密码 053

QQ会员、QQ等级任你改054

- 一、免费享受QQ会员服务054
- 二、QQ等级任你改055

获取QQ空间最高权限056

- 一、让对方用QQ邮箱作为QQ显示账号056
- 二、获取关键代码056
- 三、打开自己的QQ空间056
- 四、获取QQ空间最高权限057

当心通过邮箱盗号057

- 一、邮箱收信058
- 二、网站收信058

三、防盗技巧059

QQ聊天记录与强制聊天防范060

- 一、聊天记录安全060
- 二、强行聊天防范061

Foxmail账户破解与防范062

- 一、邮箱使用口令的安全防范062
- 二、邮箱账户密码的防范064

巧用工具拒绝盗号064

- 一、网游保镖为你护航064
- 二、用奇虎360保险箱防盗号066



第4章 加密、解密与突破

简单几步 让文件夹彻底“消失”068

- 一、更改文件夹图标068
- 二、隐藏文件名069
- 三、更改特殊文件名069
- 四、巧用“文件更名”让文件“蒸发”069

让文件阅读后自动销毁071

- 一、巧借网站实现自动销毁071
- 二、软件让你保护机密文件072

文件自动销毁也有“回天术”073

- 一、FileMon监视工具发现“真相”073
- 二、破解并提取“X-文件锁”加密的文件073

让杀毒软件“隐藏”机密文件074

- 一、文件隐藏074
- 二、机密文件提取075
- 三、机密文件不泄密075

当心系统密码被破解076

- 一、Syskey双重加密076
- 二、轻松创建“开机软盘”077

解除NOD32的密码保护077

- 一、NOD32个人密码设定078
- 二、修改注册表清除密码078
- 三、使用专用工具“解锁”078

暴力破解路由器079

- 一、暴力破解无线路由器账号、密码079
- 二、修改无线网络密码，免费蹭网080

压缩文档加密与突破080

- 一、用RAR Password Cracker恢复RAR密码080
- 二、破解压缩文件密码082

虚拟磁盘加密隐藏隐私084

- 一、创建虚拟加密磁盘084
- 二、虚拟磁盘的使用085

文件隐藏巧加密——文件隐藏大师086

一、创建隐藏文件夹	086
二、操纵“隐藏文件夹”	087
三、编辑和删除隐藏文件夹	087
四、文件隐藏大师项设置	088

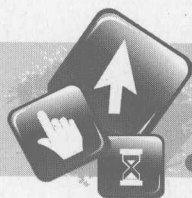
谁动了我的文件——电脑防删专家.....088

一、防止别人进行新建、复制操作	088
二、禁止改名、移动文件	089
三、禁止删除文件	089

四、设置解锁密码	089
五、查看监控记录	090
六、保护特定的文件夹	090

军用级硬盘加密.....090

一、创建虚拟磁盘空间	091
二、对数据文件加密	092
三、在虚拟磁盘创建“虚拟磁盘”	092



第5章 穿越毒笼

免费“卡巴斯基”：可牛杀毒.....093

一、双管齐下杀病毒	093
二、实时防护	094
三、网页、邮件齐监控	094

病毒木马的练兵场——虚拟机.....095

一、认识虚拟机	095
二、虚拟机安装实战	096
三、打造自己的虚拟计算机	096
四、文件共享	099
五、虚拟机中的病毒木马实战	100

大蜘蛛全方位安全保护.....101

一、大蜘蛛安装与设置	101
二、大蜘蛛安全空间杀毒实战	103
三、邮箱保护、反垃圾邮件	104
四、SplDer Gate防火墙阻断网络威胁	104
五、家长控制，上网更放心	104
六、主动防御和自我保护	105
七、资源占用	106

自己动手，打造U盘杀毒盘.....106

一、制作U盘杀毒盘	106
二、U盘杀毒盘的使用	108

抢救被杀毒软件“杀掉”的文件.....109

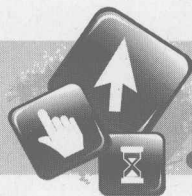
一、被杀掉的文件如何“抢救”	109
二、江民杀毒软件中如何“抢救”	109
三、瑞星杀毒软件中如何“抢救”	110
四、金山毒霸中如何“抢救”	110
五、卡巴斯基中如何“抢救”	110
六、ESET NOD32中如何“抢救”	110
七、大蜘蛛杀毒软件中如何“抢救”	111

真假Desktop.ini和*.htt文件.....111

一、病毒的入侵	111
二、网海搜毒行	112
三、清毒记	112
四、加密我的文件夹	113

打造金刚不坏之身——影子系统PowerShadow 115

一、影子系统的两种模式	115
二、影子系统危险操作测试	116



第6章 木马植入与远程控制

解析图片中如何“捆绑”木马.....117

- 一、图片与程序的“捆绑”.....117
- 二、Copy命令也来玩捆绑.....118
- 三、使用专用工具玩“捆绑”.....118

木马加壳与脱壳.....120

- 一、木马加壳的实现.....120
- 二、检测木马加壳方式.....121
- 三、原形毕露——脱壳实战.....122

影片木马攻防实战.....123

- 一、影片木马的特点.....123
- 二、RM影片木马制作.....124
- 三、RM影片木马的防范.....126

探密远程开启视频的木马.....127

- 一、远程开启视频的意义.....127
- 二、开启远程视频.....127
- 三、服务器端清除.....128

DLL木马追踪与防范.....129

- 一、动态嵌入式DLL木马介绍.....129
- 二、DLL木马的消除.....130

进程、屏幕轻松看——维度远程控制.....132

- 一、轻松配置服务端.....132

- 二、远程控制实战解析.....133

使用PcAnywhere远程控制.....133

- 一、安装设置PcAnywhere.....133
- 二、配置PcAnywhere.....134
- 三、开始远程控制.....135

用灰鸽子透过局域网进行远程管理.....136

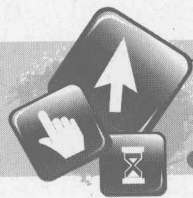
- 一、灰鸽子简介.....136
- 二、生成服务器端.....136
- 三、查看控制效果.....137
- 四、禁止灰鸽子服务.....137
- 五、彻底清除.....138
- 六、解除关联.....138

挂马网页识别、防治一手搞定.....139

- 一、什么是网页挂马.....139
- 二、网页挂马常用手段.....139
- 三、网页挂马技术解析.....140
- 四、网页挂马实战演练.....142
- 五、使用“金山网盾”防范挂马网页.....146

多种方式查杀木马——金山卫士.....147

- 一、快捷：快速修复系统漏洞.....147
- 二、双引擎：木马查杀更可靠.....148
- 三、防挂马：网页防护让你省心.....148



第7章 网吧黑客

当心局域网终结者的攻击.....149

- 一、网吧攻击原理.....149

二、局域网终结者	150
----------------	-----

网吧ARP欺骗实例151

一、欺骗原理	151
二、欺骗实例解析	151
三、ARP欺骗防范	153

网吧木马攻防实战解析.....154

一、端口映射	154
二、挂马实战	155
三、网吧木马防范	156

网吧安全上网应对之策.....161

一、场景一：诱惑的链接	161
二、场景二：强大的游戏外挂	162
三、场景三：钓鱼网站	162
四、场景四：中奖信息	163
五、场景五：黑客工具	163
六、防范之策	163

轻松突破网吧限制.....164

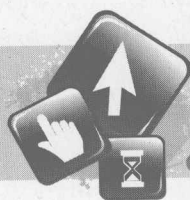
一、手工突破限制	164
二、突破注册表修改限制	165
三、“安全模式”突破法	166
四、利用工具破解	166

局域网监控大师 LanSee167

一、工具简介	167
二、搜索计算机	167
三、搜索共享资源	167
四、检查端口连接状态	168

全面封杀内网P2P——聚生网管.....169

一、破解注册很轻松	169
二、聚生网管基本配置	169
三、封杀内网P2P下载	170
四、限制使用聊天软件	170
五、限制网络流量	170
六、网络安全管理	171



第8章 漏洞攻防

Adobe Flash漏洞攻防.....172

一、入侵实战	172
二、漏洞分析与防范	173

IE7 0day漏洞攻防174

一、漏洞简介	174
二、漏洞利用代码实测	174
三、木马的利用	175
四、漏洞的防范	176

Vista输入法漏洞实战解析176

一、提权实战	176
二、安全防范	179

实战Dcom Rpc漏洞.....179

一、入侵实战	180
二、漏洞修补	181

动画光标漏洞.....181

一、漏洞入侵实战	181
二、安全防范	182

Serv-U入侵攻防183

一、准备工作	183
二、入侵实战	184

博客程序L-BLOG攻防184

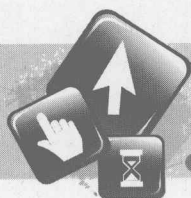
一、提权漏洞实战	185
二、漏洞分析与防范	187

Discuz模块编码漏洞利用189

一、准备工作	190
二、入侵实战	190

Excel漏洞攻防	192
------------------	------------

一、漏洞简介	192
二、入侵实战	192
三、防范策略	193



第9章 网站攻防

轻松探测网站信息	194
-----------------	------------

一、探测IP和域名	194
二、获得网站的注册信息	196
三、其它方面	197

多种手段破解网站登录口令	198
---------------------	------------

一、源代码分析破解	198
二、使用软件破解	201
三、使用注入破解	202

“一句话木马”攻防	204
------------------	------------

一、木马概述	204
二、入侵实战	205

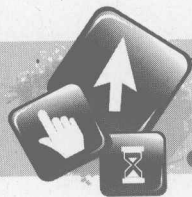
三、安全防范	207
--------	-----

PHP整站程序漏洞攻防	207
--------------------	------------

一、漏洞简介与防范策略	207
二、批量入侵实战	207

网站数据库攻防五招式	210
-------------------	------------

一、巧妙利用500错误入侵	210
二、利用关键字下载数据库	211
三、使用NBSI入侵	212
四、源代码分析	212
五、数据库防范秘技	213



第10章 服务器攻防

服务器安全隐患与入侵方式	215
---------------------	------------

一、什么是服务器	215
二、服务器入侵渠道	216

企业服务器CC攻击实战解析	217
----------------------	------------

一、攻击原理	217
二、攻击实例解析	218

三、识别CC攻击	220
----------	-----

巧设规则轻松抵御CC攻击	220
---------------------	------------

一、第一条规则	221
二、第二条规则	221
三、第三条规则	222
四、第四条规则	222

DDoS攻击实战解析223

- 一、DDoS攻击原理 223
- 二、攻击实例剖析 223
- 三、识别DDoS攻击 224

DDoS防范与反击225

- 一、防范措施 225
- 二、反击策略 225

服务器漏洞攻防227

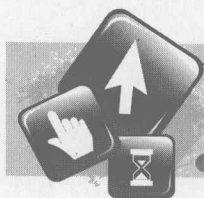
- 一、攻击原理 227
- 二、攻击实例 227
- 三、安全防范 230

数据库攻防之道231

- 一、数据库概述 231
- 二、攻击实例之SQL溢出 232
- 三、实例攻击之SQL弱口令 233
- 四、实例攻击之SQL 2005注入 234

服务器安全配置235

- 一、安装补丁 235
- 二、杀毒软件 237
- 三、权限设置 238
- 四、删除LAN设置 239



附录 黑客常用的命令工具

攻防命令之Arp241

攻防命令之AT242

攻防命令之Del和RD244

攻防命令之Gettype和Systeminfo245

攻防命令之Ipconfig246

攻防命令之Netstat246

攻防命令之Ping247

攻防命令之Nslookup249

攻防命令之Net250

第1章 扫描、嗅探与欺骗

很多恶意程序都会很不客气地加入到系统的启动项中，进而导致系统变慢、数据被窃取等问题涌现。那么，这些恶意程序都是怎样成为启动项目的？怎样才能把这些不懂礼貌的家伙赶出去？这里，就将为读者们剖析 Windows 中的扫描、嗅探与欺骗。

X-scan查看电脑隐患应用实例

X-scan 作为国内最著名的扫描软件，相当多的安全爱好者都在使用它来对特定主机进行漏洞扫描与探测。但你想过吗？X-scan 也是可以用在自己的计算机安全管理上的——正如一把枪，到了战士手里就是保家卫国的武器；到了歹徒手中却成了行凶作恶的工具！

利用 X-scan，可以高效实现本机的安全漏洞探测，从而使本机的安全管理变得轻松起来！

一、X-scan简介

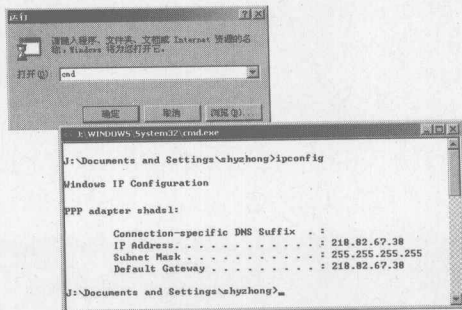
X-scan 可以安装在 Windows NT4/2000/XP/2003 上，其采用的多线程方式可以对指定 IP 地址段（或单机）进行高速的安全漏洞检测，它提供了图形界面和命令行两种操作方式，扫描内容包括：远程服务类型、操作系统类型及版本，各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等二十几个大类。对于多数已知漏洞，X-scan 给出了相应的漏洞描述、解决方案及详细描述链接……

二、X-scan的基本使用

X-scan 提供了图形界面和命令行两种操作方式，相对于初学者来说，直观明了、简单易学的图形界面操作显然是最适合不过的了。所以下面将着重讲解图形界面下的使用方法。

1. 查知本机IP地址

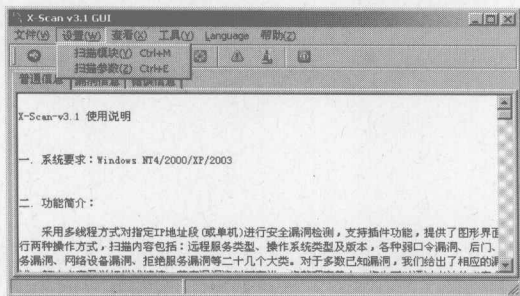
首先需要指定扫描的 IP 范围。由于是探测本机，所以应首先在“运行栏”中输入“Cmd”命令打开“命令提示符窗口”，在命令行中输入“IPconfig”命令，来查知本机的当前 IP 地址。



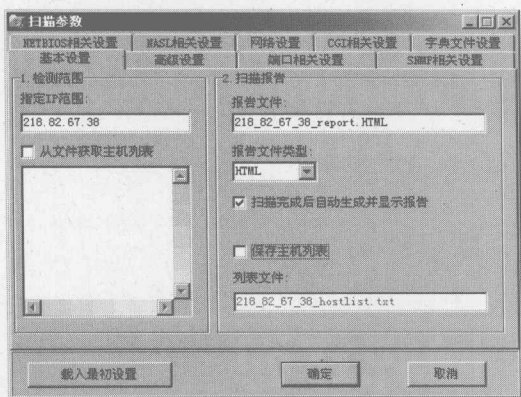
从返回的信息可以看出，当前本机的 IP 地址为“218.82.67.38”。

2. 添加IP地址

在得到了本机的 IP 地址后，现在就可以在 X-scan 主窗口点击“设置”、“扫描参数”菜单项，准备把 IP 地址添加到 X-scan 中了。



在接着弹出的“扫描参数”对话框中，在“指定 IP 范围”右侧的文本框中输入 IP 地址（如 218.82.67.38）或域名。



提示 // ATTENTION

在“指定 IP 范围”项的文本框中，除了可以输入单个的 IP 地址外，也可以输入以“-”和“,”分隔的 IP 范围，如“192.168.0.1-192.168.0.20;192.168.1.10-192.168.1.254”，这样就可以实现某个较大范围的 IP 地址输入了。

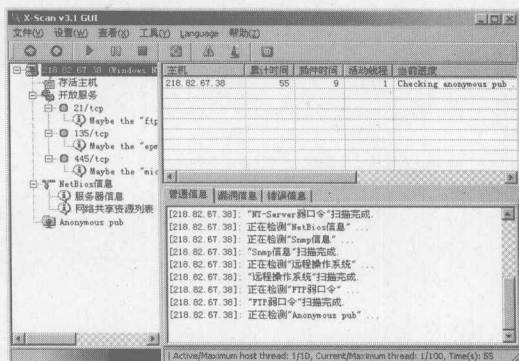
除了手工输入扫描范围外，还可以通过选中“从文件中获取主机列表”后，从存储有 IP 地址的文本文件中读取待检测主机地址，要注意的是：在文本文件中，每一行可包含独立 IP 或域名，也

可包含以“-”和“,”分隔的 IP 范围。

在 IP 地址输入完毕后，可以发现扫描结束后自动生成的“报告文件”项中的文件名也在发现相应的变化。通常这个文件名是不必去手工修改的，我们只需记住这个文件将会保存在 X-scan 目录的 LOG 目录下就可以了。设置完毕后，点击“确定”按钮关闭对话框。

3. 开始扫描

在返回到 X-scan 主窗口后，只需按“Ctrl+S”键即可开始对指定 IP 进行安全扫描了。由于 X-scan 是采用多线程对目标进行扫描的，所以扫描的速度将会非常快。



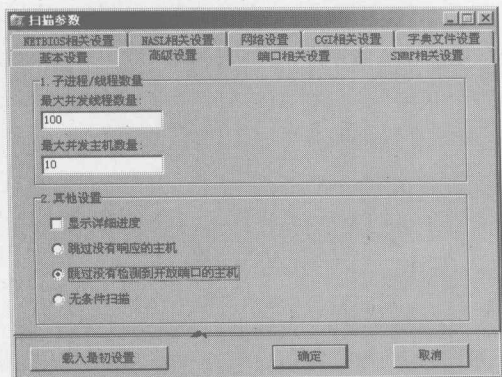
从上图可以看出当前计算机开放了三个端口，其中就有目前受病毒冲击最利害的 135 端口在开放。此时快采取打补丁等措施关闭 135 端口吧！

三、高级设置

X-scan 的使用是很容易的，但缺省状态下它的效果却往往不会发挥到最佳状态，这个时候就需要进行一些高级设置来让 X-scan 变得强大起来——需要注意的是，高级设置需要根据实际情况进行设定，否则 X-scan 也许会因为一些“高级设置”而变得脆弱不堪，如毫无反应了！

1. 跳过没有检测到开放端口的主机

这个选项的意思是：若在用户指定的 TCP 端口范围内没有发现开放端口，将跳过对该主机的后续检测。这个选项中，可以大大提高 X-scan 批量扫描时的效率。



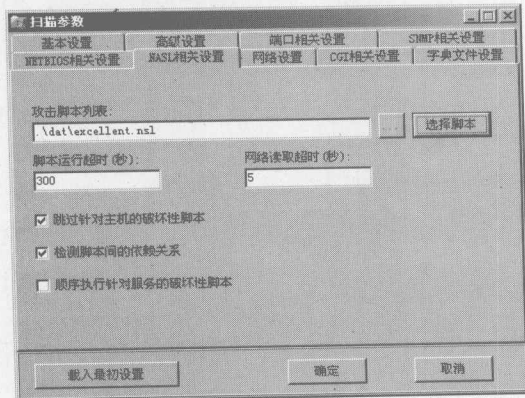
提示 ATTENTION

因为计算机对外进行的一切操作都需要有个相应开放的端口才能进行，所以没有检测到端口开放的主机，已经毫无意义了，所以可以选择跳过。

2. 设置攻击脚本列表

由于目前 Scripts 目录中的脚本数量已近 2000 个，在批量扫描中可以通过定制脚本列表，只选取高风险级别漏洞进行检测，以加快扫描速度。

在“扫描参数”对话框中，点击切换到“NASL 相关设置”选项卡设置界面。

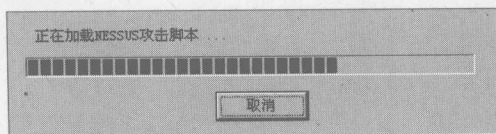


请注意，这里的“检测脚本间的依赖关系”项，是指 NASL 脚本间相互是有关联的，比如一个脚本先获取服务的版本，另一个脚本再根据服务版本进行其他检测。如果打乱了脚本的执行顺序可能会影响扫描结果，但也由于脚本间不需要互相等待，会节省扫描时间。

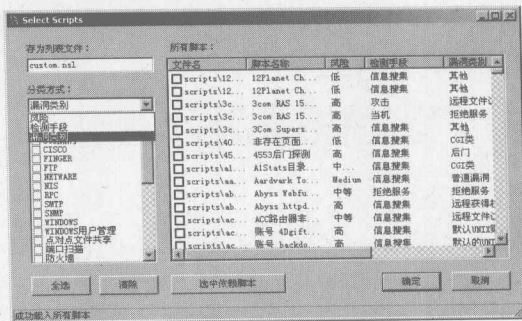
而“顺序执行针对服务的破坏性脚本”项，

则是指如果一个脚本正在尝试某个服务，另一个脚本同时在获取该服务信息，或同时有其他脚本尝试溢出该服务，将导致扫描结果不正确。但如果脚本间不需要互相等待，将会节省扫描时间。

因为要设置攻击脚本列表，所以此时应点击“选择脚本”按钮，稍后程序将自动开始脚本的加载操作。



在加载完毕后打开的脚本选择窗口中，可以通过“风险”、“检测手段”、“漏洞类型”等分类方式定制脚本列表。

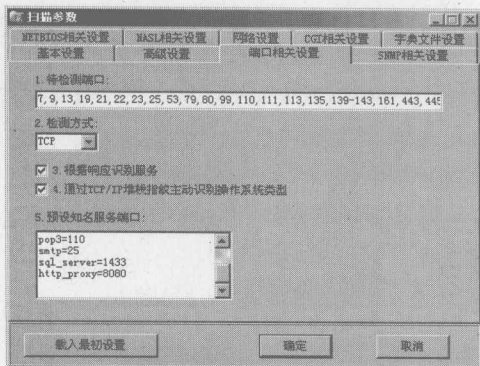


设置完毕后，点击“确定”按钮关闭脚本选择窗口。

3. 设置扫描端口

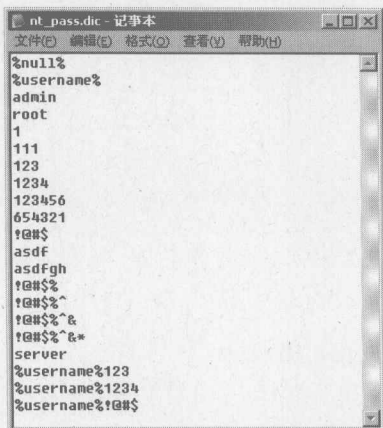
端口是扫描中用于识别主机是否存在安全漏洞的重要依据，我们可以根据端口号的不同，识别出系统开的服务或安装了哪些软件。一位有经验的黑客，则可以据此迅速判断出入侵的最佳入口所在！之所以要设置扫描端口，是因为随着系统服务可能出现的安全漏洞增加，X-scan 默认开放的端口往往不能满足安全检测的需要，所以此时就需要对端口进行添加等设置了。方法如下：

在“扫描参数”对话框中点击切换到“端口相关设置”选项卡设置界面，在“待检测端口”项中可以手工输入单个端口或以“110-150”这样的方式输入批量端口。



4. 更换字典

字典是 X-scan 用来尝试暴力猜解主机是否存在弱口令用的。在 X-scan 中，默认的字典文件有很多，但如果你使用“记事本”程序打开 X-scan 的“dat”目录下以 dic 后缀名存在的字典文件（如 nt_pass.dic）的话，就会发现字典中的默认字词量还是太少了。

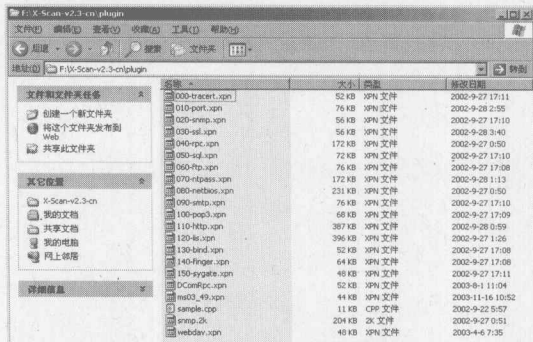


此时，请使用“万能字典”等程序生成符合要求的字典文件后，将字典文件保存到 X-scan 的“dat”目录下，接着要更改生成的字典文件名。如生成的字典文件名为 abc.dic，这个字典文件打算替代 X-scan 下的 nt_pass.dic 文件，那么 abc.dic 文件名就应该改成 nt_pass.dic 文件名，并将原 nt_pass.dic 文件删除即可。

5. 安装插件

插件如同 Photoshop 的滤镜，熟悉图形处理的朋友都会知道滤镜可以使图形处理变得轻松自如且效果惊人。而插件则可以使 X-scan 变得功能无穷，如可以扫描的服务原来是 100 项，在使用插件后也许就可以达到 1000 项！在 X-scan 中安装插件的方法如下：

首先在各大网站下载 X-scan 的插件，如在 <http://www.xfocus.net/tools/200307/488.html> 中下载“DComRpc.xpn”插件后，再将该插件复制到 X-scan 的“plugin”目录下就可以了。



国产第一扫描器“流光”

流光在国内的安全爱好者们眼中可以说是无人不晓，它不仅是一个安全漏洞扫描工具，更是一个功能强大的透渗测试工具。流光以其独特的 C/S 结构设计的扫描设计颇得好评。

一、流光简介

流光 5.0 必须运行于 Windows 2000 或

者 Windows NT 系统中，并且内存应尽可能地不要小于 128MB。目前流光的功能已经颇为全面，它可以扫描的漏洞有：POP3、FTP、IMAP、TELNET、MSSQL、MYSQL、WEB、IPC、RPC、DAEMON 等；

暴力猜破出：POP3、FTP、IMAP、HTTP、PROXY、MYSQL、SMB、WMI 等密码；