电脑报 总策划

黑客

致命絕殺

88种兵器全解析

工具·进阶篇

仲治国 白海峰 编著

揭秘88种常用兵器
完全黑客攻防精通

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

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

电脑报电子音像出版社
CPCW Electronic & Audiovisual Press

黑客

致命絕殺

88种兵器全解析

工具进阶篇

仲治国 白海峰 编著

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

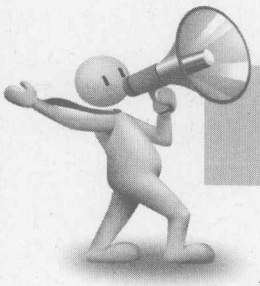
版权所有　盗版必究
未经许可　不得以任何形式和手段复制和抄袭

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！

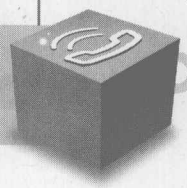
黑客88种兵器全解析

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
CD生产：四川省蓥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。

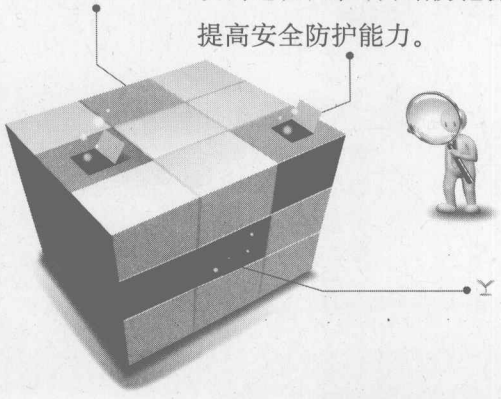
正所谓兵来将挡，水来土掩。只要我们抱着“勿恃敌之不来，恃吾有以待之”的精神，必能将各种危机化解于无形！熟读兵书三百遍，不会用兵也能防。

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。

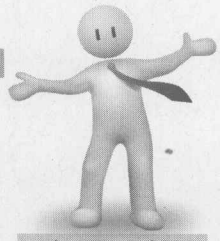
《黑客 88 种兵器全解析》：精选了黑客最常用的 88 种攻防工具，通过工具的实战操作帮助读者快速领悟黑客攻防手段。

《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

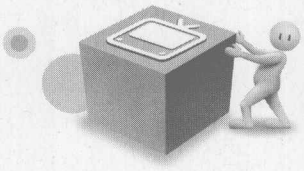
2010 年 9 月



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。



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

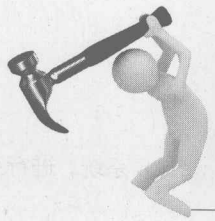
黑客绚丽屏保

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

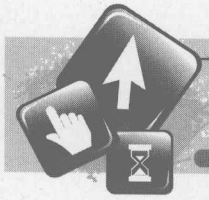
第 1 章 扫描嗅探与欺骗
第 2 章 进程与端口攻防
第 3 章 直面网络盗号
第 4 章 加密、解密与突破
第 5 章 穿越毒龙
……

此为试读，需要完整PDF请访问：www.ertongbook.com

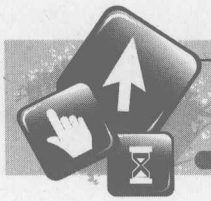


目录 CONTENTS

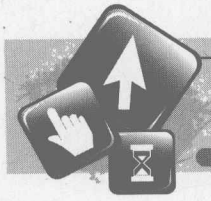
致命绝杀
黑客88种兵器全解析



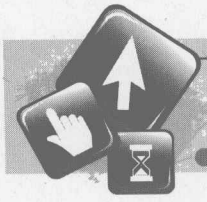
第1章 扫描、嗅探与欺骗



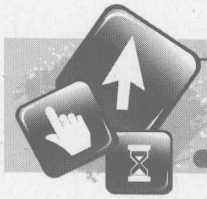
第2章 进程与端口攻防



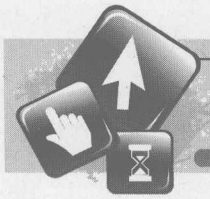
第3章 直面网络盗号



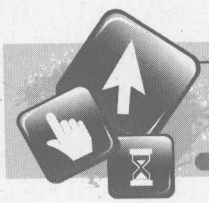
第4章 加密、解密与突破



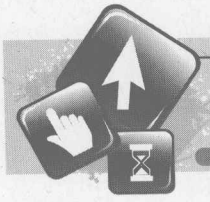
第5章 穿越毒笼



第6章 木马植入与远程控制

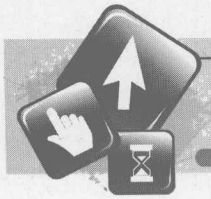


第7章 网吧黑客

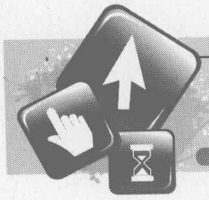


第8章 漏洞攻防

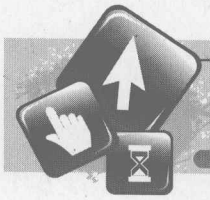
此为试读，需要完整PDF请访问：www.ertongbook.com



第9章 网站攻防



第10章 服务器攻防



附录 黑客常用的命令工具

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

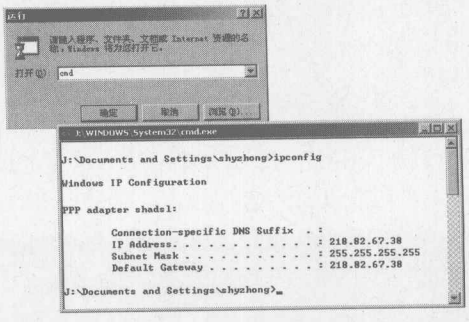
X-scan 可以安装在 Windows NT4/2000/XP/2003 上，其采用的多线程方式可以对指定 IP 地址段（或单机）进行高速的安全漏洞检测，它提供了图形界面和命令行两种操作方式，扫描内容包括：远程服务类型、操作系统类型及版本，各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等二十几个大类。对于多数已知漏洞，X-scan 给出了相应的漏洞描述、解决方案及详细描述链接……

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

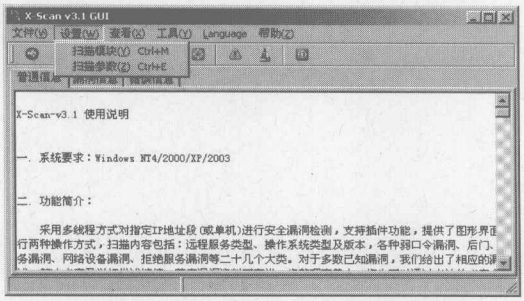
首先需要指定扫描的 IP 范围。由于是探测本机，所以应首先在“运行栏”中输入“Cmd”命令打开“命令提示符窗口”，在命令行中输入“IPconfig”命令，来查知本机的当前 IP 地址。



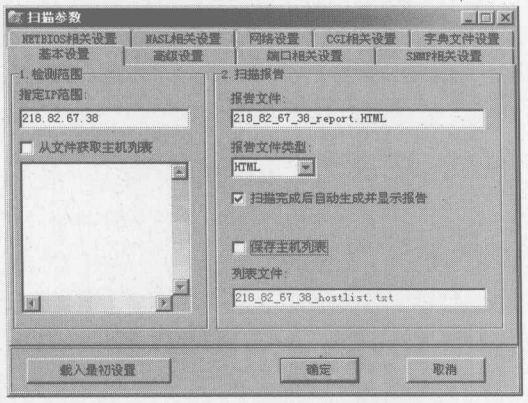
从返回的信息可以看出，当前本机的IP地址为“218.82.67.38”。

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

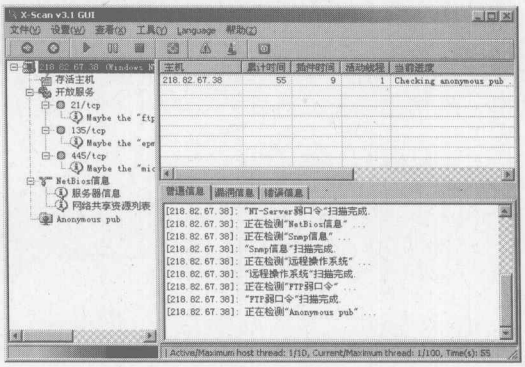
在“指定IP范围”项的文本框中，除了可以输入单个的IP地址外，也可以输入以“-”和“,”分隔的IP范围，如“192.168.0.1-192.168.0.20,192.168.1.10-192.168.1.254”，这样就可以实现某个较大范围的IP地址输入了。

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。



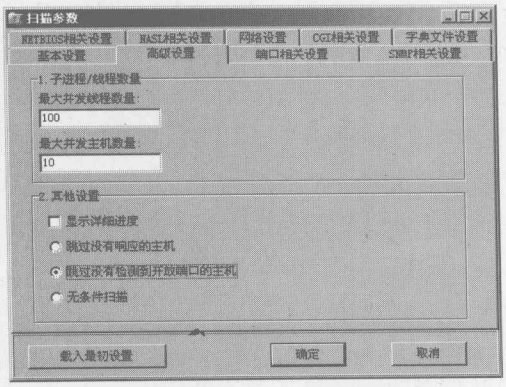
从上图中可以看出当前计算机开放了三个端口，其中就有目前受病毒冲击最利害的135端口在开放。此时快采取打补丁等措施关闭135端口吧！

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。



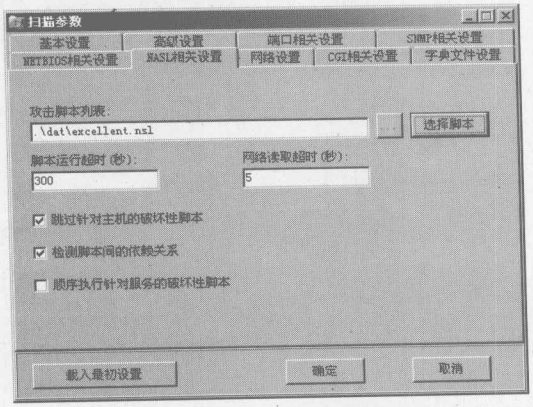
提示 ATTENTION

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。

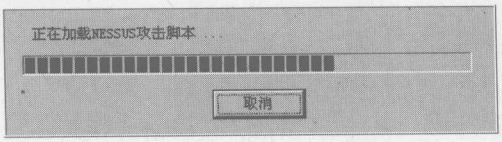
在“扫描参数”对话框中，点击切换到“NASL 相关设置”选项卡设置界面。



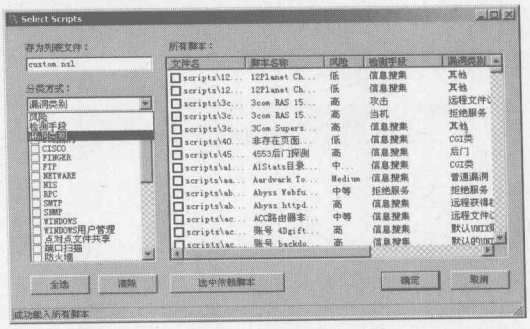
请注意，这里的“检测脚本间的依赖关系”项，是指 NASL 脚本间相互是有关联的，比如一个脚本先获取服务的版本，另一个脚本再根据服务版本进行其他检测。如果打乱了脚本的执行顺序可能会影响扫描结果，但也由于脚本间不需要互相等待，会节省扫描时间。

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。

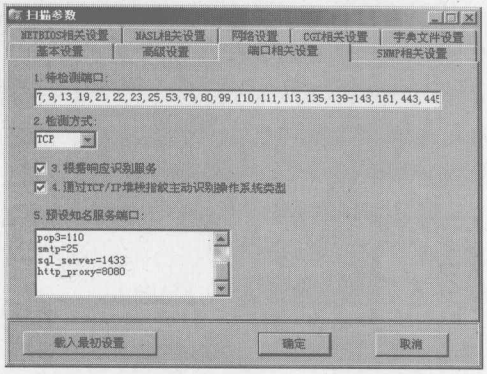


设置完毕后，点击“确定”按钮关闭脚本选择窗口。

3. 设置扫描端口

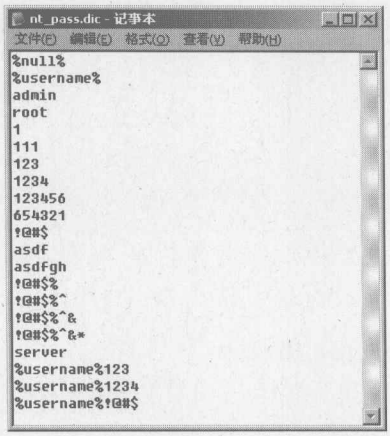
端口是扫描中用于识别主机是否存在安全漏洞的重要依据，我们可以根据端口号的不同，识别出系统开的服务或安装了哪些软件。一位有经验的黑客，则可以据此迅速判断出入侵的最佳入口所在！之所以要设置扫描端口，是因为随着系统服务可能出现的安全漏洞增加，X-scan 默认开放的端口往往不能满足安全检测的需要，所以此时就需要对端口进行添加等设置了。方法如下：

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。

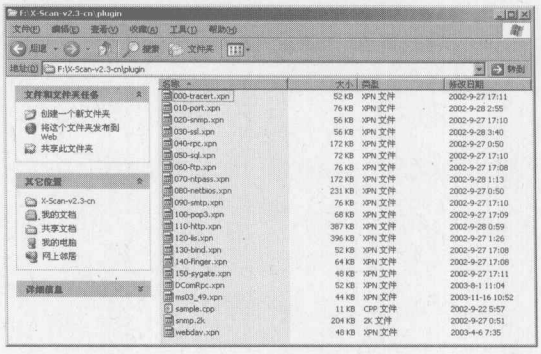


此时，请使用“万能字典”等程序生成符合要求的字典文件后，将字典文件保存到X-scan的“dat”目录下，接着要更改生成的字典文件名。如生成的字典文件名为abc.dic，这个字典文件打算替代X-scan下的nt_pass.dic文件，那么abc.dic文件名就应该改成nt_pass.dic文件名，并将原nt_pass.dic文件删除即可。

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；

此为试读，需要完整PDF请访问：www.ertongbook.com