黑客X档案 •优秀图书•
Hacker X Files

黑客兵器谱II

121个hack小工具教程+X档案黑刀推荐十大工具深度全曝

¥ 22.00

《黑客X档案》图书邮购信息

双CD+双图书=28.8元

CD+双图书=19.00元

CD+图书=25.00元

CD+图书=12.00元

CD+图书=19.00元

菜牛哥哥动画教你学Hack

CD+图书=10.00元

杂志邮购信息：

2003年——1期，5期，6期，[illegible]期,9期，10期，11期，12期
单价：8.8元

2004年——1期，2期，3期，[illegible]期，5期,6期 单价：9.00元

邮购时请注明书名、邮编、详细地址、电话和姓名，为[illegible]一律挂号邮寄，请加寄挂号费[illegible]元，建议加挂号。

读者服务部电话：010—88560080
邮购地址：北京市海淀区增光路45号
邮购联系人：小邵
收信人：《黑客X档案》邮购部
邮编：100037

黑客X档案
HackerXFiles

作 者：
杨东柱（sagi）
裴 信（雪莲蓬）
汪利辉（iceyes）
梁 伟（Python）

做一本和读者躺着看的杂志

不让生活磨灭我们的个性

平民化 自由度 随意性突破极限

拥有国内人气指数最高的黑客类媒体 www.hackerxfiles.net

黑客兵器谱II

黑客兵器谱II

出版：吉林科学技术出版社

出品人：孙胜利

主编：覃华

编辑部主任：孙志强

编辑部：Zero 黑裤子 土豆 呆呆虫 楚汉 Sagi

特约编辑：Python 射手 雪莲蓬 ICEYES

光盘部：龚连成

美编：何有接 Bifrost

排版：何有接

E-mail:hackerxfiles@263.net

邮购查询E-mail:chaxunx@263.net

读者服务部电话：（010）88560080

发行电话：（010）88561472

发行联系人：赵琦 小邵

邮编：100037

定价：22.00元（双光盘+手册）

前　言

倘若上帝愿意给你一个可以登上天堂的天梯，你是否仍然执意的要自己去花N年的时间去另外造一个呢？有许多网络高手，经常嘲笑那些只会使用工具的网络新手们，或许他们也忘记了，他们刚开始接触网络安全时，也是这么过来的，而且他们即使是现在，也仍然在使用着别人的工具，只是工具不同罢了。我想不出使用工具有什么不好，更想不出拒绝使用这些工具的任何理由，让我们站在巨人的肩膀上吧，我们会看得更远、更高。

本书面向的读者

如果你对于网络安全感兴趣，而又是一个刚刚接触这方面知识的新手的话，我们建议你祥细的阅读本书，学习各种网络安全工具的应用，而如果你自栩已经是这方面的高手的话，那么，请略过此书。

本书的章节分类 ▼

本书以介绍网络安全工具的使用为主，全书共分为七个章节：第一章，主要介绍了网络安全检测（扫描）工具的使用；第二章，主要介绍了两款常用的远程控制程序的使用；第三章，主要介绍了远程溢出攻击程序的使用；第四章，介绍了黑客在入侵过程中常用的一些辅助工具；第五章，主要介绍了一些常用的后门工具的使用；第六章，介绍了几款嗅探（sniffer）工具的使用；第七章，以介绍其他的综合工具为主。

本书中所涉及的所有工具，都是基于Microsoft Windows系统平台的，我们强烈建议你使用Windows 2000/xp/2003系统，因为其中的一些工具程序是无法在Windows 9*/ME系统下来运行的。限于某些原因，对于一些商业程序或注册程序的破解类工具以及特洛伊木马程序的使用我们没有做介绍，就连远程控制类的工具，我们也只是简单的介绍了最常用的两款。另外，就是针对Unix/Linux系统的安全工具，我们也没有涉及，只是在第三章，也就是远程溢出攻击程序的使用的一章中，简单的介绍了几个。

在实际的应用中，我们希望读者可以理论结合实践，灵活的运用各种工具，再结合操作系统本身的一些特性，而并非是单纯的依靠这些工具程序。举个简单的例子，当我们利用对方系统上存在的安全漏洞入侵了对方的系统后，成功的在对方的系统中添加了一个具有管理员权限的后门帐号，也开启了对方的远程登录（telnet）服务，那么此时我们通常的做法是使用ntlm.exe或是opentelnet来清除对方的ntlm验证，但实际上我们不使用任何的工具也可以绕过对方的ntlm验证来成功的登录，我们只需要在自己的系统上添加一个和对方一模一样的帐号，然后以该帐号登录自己的系统，或是以该帐号身份来运行cmd，那么，在该cmd窗口下使用telnet客户端程序就可以直接登录对方的系统，而绕过对方系统的ntlm验证了。

光盘说明 ▼

本书中所有涉及的工具都已收录在了第一张光盘中，另外，在第一张光盘中，我们还整合了许多其他经典的工具程序，可以说包括了网络安全的方方面面，包括windows 2000 终端服务（3389）的远程溢出工具、Linux telnet的远程溢出工具、Linux gopher 2.3.1的远程溢出工具、BSD telnet的远程溢出工具、AIX infod的远程溢出工具、SunOS sadmind的远程溢出工具、基于Windows 系统平台的apache 1.3.*的远程溢出工具、ws-ftp的远程溢出工具、wu-ftp的远程溢出工具、各种网页木马、黑洞2004、灰鸽子、广外幽灵、radmin、lecher、Recub、URC、zxshell等远程控制（木马）程序等。在第二张光盘中我们主要收录了一些安全方面的动画教程，或许这种有声有色的动画，也会让你在学习的同时体会到许多的乐趣吧。

注意事项 ▼

本书所介绍的工具程序，有许多都带有恶意的攻击性，可能会给你的测试目标带来很大的危害，因此我们希望你能够慎重的使用这些工具，由此而带来的所有后果，均由测试者本人承担！

感谢 ▼

在这儿特别感谢动画教程的提供者——怪狗（http://www.77169.com），也感谢所有支持过我们，帮助过我们的朋友！

雪莲蓬、Python、sagi、iceyes

一、扫描

【致命前奏】

二、远程控制

【秘密潜入】

三、远程溢出

【刺穿你的防线】

四、入侵辅助

【无声配角】

光盘A

文章所涉工具介绍

X-Scan 强大的扫描工具。采用多线程方式对指定IP地址段(或单机)进行安全漏洞检测，支持插件功能，提供了图形界面和命令行两种操作方式。

X-way 可对系统进行综合扫描，包括端口扫描，系统CGI漏洞扫描，包括搜集的1000多条CGI漏洞等。

nmap 被开发用于允许系统管理员查看一个大的网络系统有哪些主机以及其上运行何种服务。

ASC 扫描ASP文件是否存在注入点。

SleuthSetup 网页文件检查工具，可检查的文件类型很多，如ASP、JSP等。

sql2.exe ms-sql的溢出工具。

thcsql 针对MSSQL OpenDataSource函数漏洞的攻击程序。

aspcode.exe ASP溢出工具。

rpc_locator.exe&rpc.exe RPC LOCATOR溢出。

rpcloname: Rpcdcom 长文件名的远程溢出。

realex.exe Real server的远程溢出。

msghack.exe Windows messenger服务的远程溢出。

ms03049 Ms03-049的远程溢出。

winfp30reg2 Frontpage fp30reg.dll的远程溢出。

ms04011lsass Ms04-011 Lsasrv.dll RPC远程溢出。

sun.exe SUNOS telnet远程溢出程序。

irixtelnet.exe IRIX telnet远程溢出程序。

0x333samba.exe LINUX SAMBA的程序。

Servu5.0.0.4.rar Servu FTP 5.0.0.4的远程溢出。

SqlInj.exe 脚本注入自动攻击程序。

mport.exe CMD下列举打开端口的文件。

AProMan 一个2000/XP下基于命令行的进程工具，可查看进程，端口进程关联关系。

gina.exe 木马的主要作用是在系统用户登陆时，将用户登陆的名字、登陆密码等记录到文件中去。

NTSHELLGINA.DLL 图形界面下记录登录密码。

klogger.exe 一个几kb的击键记录工具。

whoami.exe 察看当前用户名称等。

erunasx DEBUG漏洞的本地溢出。

winwmiex wmi server的本地溢出。

xdebug windows kernel本地溢出。

local04011ex MS 04-011的本地溢出。

PortlessNew 一个使用svchost.exe去启动、平时不开端口、可以进行反连接的后门程序。

dtx3389.bat 远程开3389。

Cmdasp.asp asp的后门。

MYdoom mydoom后门的利用程序。

sasserftp sasser振荡波病毒利用程序。

GUIControlTelnet 图形界面下远程开启、关闭Telnet服务的工具。

iCmd.exe Windows下一个很小巧的后门工具。

hxdef100.rar 优秀的后门程序—黑客守卫者。

icmpdoor.rar WinNT\2000\XP下的一个很好的ICMP后门。

T-Sniffer GUI界面的嗅探器工具，支持TCP/UDP/ICMP协议数据包的捕获。

winsniff 有强大的处理功能，它能找出POP3/TELNET/HTTP/FTP/IMAP/NNTP的口令，并且它能用unix信箱格式保存所有邮件消息。

xsniff 简易的命令行方式嗅探器。

xport 多线程方式扫描目标主机开放端口，扫描过程中根据TCP/IP堆栈特征被动识别操作系统类型。

PortMap 能将机器的端口号TCP/UDP映射到其它的机器或其它IP地址上，支持来访IP的访问控制，停留在system tray上，非常不错的软件。

PEiD 现在软件越来越多的加壳了，给破解带来非常大的不便，但是这个软件可以检测出450种壳，非常方便。

pe-scan 可以测出壳的种类很多，还可以测出壳入口点、偏移量及pep。

ASProtect 功能非常完善的加壳、加密保护工具。能够在对软件加壳的同时进行各种保护。

PwDump3.exe 能从一台远程Windows服务器上获取密码hash而不管是否安装了syskey。

LC5 口令破解工具。

john 大名鼎鼎的john FOR windows版本！unix密码破解的老大。

pstools系列 系列工具包括：远程登陆、杀死进程等12个小工具。

ldapbrowser253 ldap服务的远程连接管理程序(389端口)。

兵器推荐介绍

explore2fs explore2fs就像是一个explorer，能读取你的Linux等下ext2fs分割区的软件。

JAVA JSP/JAVA环境架设程序集合。

VB6精减版 8MB，可谓短小精悍。

ermeo-securitydriver 将应用程序的TCP网络连接请求转换成sock请求发送出去。

Net Tools X 一款简单易用而功能强大的网络工具，集合了各种常用的网络监测和扫描功能。

Sasser Scanner ms04011 lsasrv扫描器。

多功能密码破解软件3.0

winapache.pl 于Windows系统平台的APACHE 1.3.*的远程溢出程序。

ws-ftp WS-FTP的远程溢出程序。

aix Aix 3.4 infod的远程溢出程序。

BTDWV04182004GB.exe 下载Torrent文件格式的程序。

Dtxtelnet11 基于BAT文件格式的远程开启TELNET的程序。

hpjetroot.pl HP jetroot的远程溢出程序。

linuxmodgzip Linux modgzip的远程溢出程序。

linuxtelnet Linux telnet远程溢出程序。

Media新溢出 针对WIN 2000 SP4的Media的远程溢出程序。

网页木马 包括ASP、PHP、JSP和PERL的网页木马。

snd-cracked 用于破解WINRAR压缩文件的密码。

thcbindinfo.exe 远程检测BIND版本信息的工具。

tsr3389.exe WIN XP远程桌面连接的安装程序。

WebDataAdmin.msi 微软发布的基于ASP.net平台下的MS SQL的远程管理程序。

winimailex.exe Imail的远程溢出程序。

winisspam Windows ISSPAM远程溢出程序。

光盘B

脚本入侵

三分钟入侵WEB站点
SQL动网漏洞之直接提升管理员
SQL跨库查询
SQL注入过程
SQL注入基础
SQL注入实战
动网7upfile漏洞
黄金眼配合注入
强制控件网页木马动画教学
入侵动力文章
入侵动网7sp2以下任意版本
用脚本来上传文件

破解实战

Netsuper的解除运行次数的限制
pc掌中宝
破解不让复制文章
破解光驱精灵
破解幻影
破解木马终结者
破解压缩密码zip
如何拷贝光盘中隐藏目录中的文件
软件如何脱壳

黑客基础

IE进行远程控制
IIS.asp映射分块编码远程缓冲区溢出
Media的远程溢出
MS04-011介绍
安装linux
破解FTP帐号

网管路由

安装DNS支持AD
登陆到路由
简简单单玩路由
配置、管理Exchange 2000 Server
配置SMTP、POP3、IMAP虚拟服务器
CISCO IS-IS路由系统讲座
tcp-ip教学

编程讲座

JAVA编译解释
Perl编译程序
SQL的SELECT
VB平方计算
VC渐变背景对话框

精彩放送

4分钟学会汉化软件
Linux管理系统服务
Linux下MV命令的使用方法
打造自己的logo
最小的asp后门演示动画
让初级黑客对您电脑扫描无用武之地
QQ2004版如何免费建群
动网upload漏洞

第一章

扫描

致命前奏

网络安全检测（扫描）工具，可以说是整个网络安全中最重要的了，它就象一把双刃剑，管理员使用他们，可以发现自己系统上存在的安全脆弱点，而对于入侵者来说，这些工具却同样可以让他们得到目标主机上足够的信息，甚至是各种安全漏洞。

本章节主要介绍目前国内网络安全爱好者中广泛使用的非商业版本的几款安全检测（扫描）工具。

1.1 X-Scan 3.1

X-Scan 3.1 X-Scan 3.1 X-Scan 3.1 X-Scan 3.1 X-Scan 3.1 X-Scan 3.1 X-Scan 3.1 X-Scan 3.1 X-Scan 3.1 X-Scan 3.1 X-Scan 3.

x-scan3.1是x-scan的最新版本，修正了3.0及3.02版本中的一些的小的BUG，在新的3.1版本中仍然和3.02版本一样使用了相对稳定的WinPCap的2.3版本，另外，主要是针对Update.exe、nessus攻击脚本、cgi漏洞库等进行了升级。

与早期的x-scan2.3相比，我认为新版本的改动主要有以下几个主要的方面，一个是增加了在线升级功能，我们只需要运行x-scan目录下的Update.exe程序或者是点击x-scan3.1图形界面上的“在线升级”按钮，就会自动的连接升级服务器（默认为安全焦点的服务器），检测是否有更新的版本，如果没有的话，会提示我们当前的就是最新的，如果有的话就会提示我们进行升级，见图1。

图1

整个升级过程都是自动的，不需要我们进行干预。另外一个比较大的改动应该是多了Nessus攻击脚本的检测，这使得x-scan3.*在某些方面越来越象Unix/Linux系统下大名鼎鼎的扫描程序Nessus了，虽然针对远程Unix/Linux系统的扫描而言，x-scan3.1似乎还无法与Nessus相比，但无论如何比起前期版本已经提高了许多。另外就是升级了cgi漏洞列表库，对于远程主机的操作系统使用了TCP/IP堆栈指纹，这也使得对于远程主机的操作系统判断的更加准确了。另外还有一些改动，我想各位在使用中就能感觉到了。

x-scan3.1运行后的主界面如图2所示，同前期的2.3版本相差不大，上方的按钮依次为：“扫描模块”、“扫描参数”、“开始扫描”、“暂停扫描”、“终止扫描”、“检测报告”、“使用说明”、“在线升级”、“退出”。

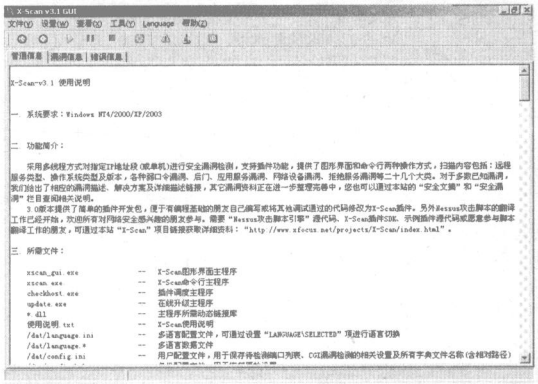

图2

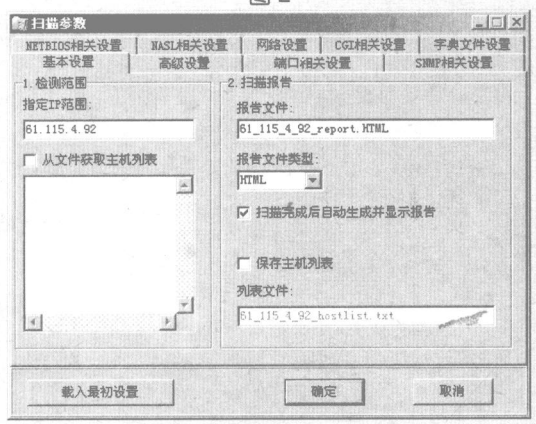

图3

我们点击“扫描参数”，打开扫描参数设置的

菜单，见图3，在“基本设置”菜单中我们在“指定IP范围”栏中输入要检测的目标主机的域名或IP地址，可以对单个目标进行检测，也可以对多个目标进行检测，例如输入“**192.168.0.1-192.168.0.254**”，这样，x-scan3.1就会对整个网段的主机进行检测了。

在“高级设置”菜单中我们通常需要设置的是“跳过没有响应的主机”或“无条件扫描”，如果选择“跳过没有响应的主机”，那么对于禁止ping或者是因为远程主机防火墙设置而致使没有响应的，x-scan3.1就会自动的跳过去，检测下一台主机，如果选择“无条件扫描”的话，见图4，x-scan3.1将会使用一些复杂的技术来对目标进行祥细的检测，虽然检测会更加的准确，但同时扫描的时间却也非常的长。因此，到底在速度及准确性上选择哪一个就看你自己了，我的做法通常是针对单个的目标主机时，选择“无条件扫描”方式，而如果扫描一批主机时选择“跳过没有响应的主机”。

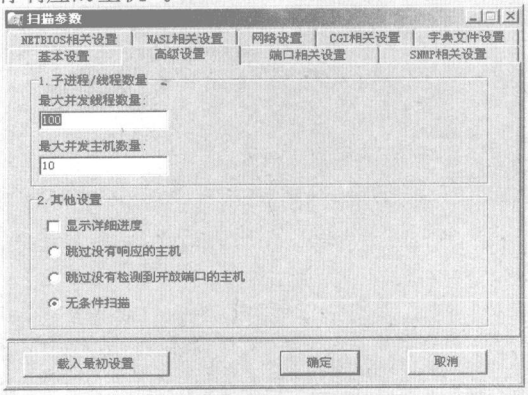

图4

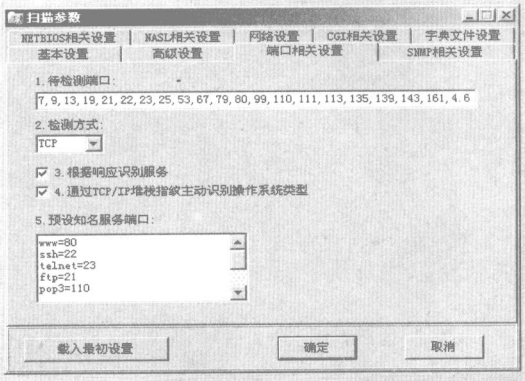

图5

在“端口相关设置”中，见图5，我们可以自由的定义需要检测的端口，当然你可以输入“1-65535”来扫描所有的端口，如果你的时间很充足的话。在“检测方式”中我通常是选择“SYN”方式。

在“SNMP相关设置”中，主要是针对SNMP信息的检测设置，图6。

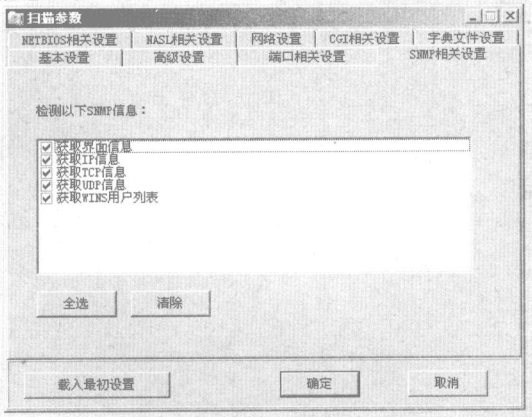

图6

在“NETBIOS相关设置”中主要是针对WINDOWS系统的NETBIOS信息的检测设置，包括的检测项目很多，我们可以根据需要来进行选择，图7。

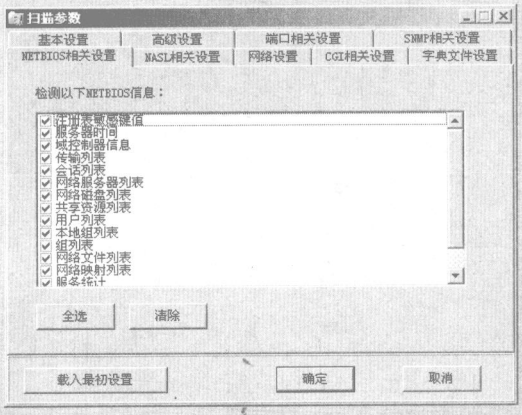

图7

在“NASL相关设置”中，有一些检测脚本对于远程主机是有破坏性的，也许会造成远程主机上的某些服务的异常中止，这样当然会很容易的暴露自己，因此你可以根据自己的需要来进行选择，见图8，xscan3.1中默认使用的攻击脚本为“excellent.nsl”，我们可以点击右边的“选择脚本”，在“漏洞类别”中选择一些比较严重的安

全漏洞，这样针对该漏洞的nessus攻击脚本就会被选中，我们就可以相对快速的检测特定的安全漏洞，当然我们也可以全部选中，不过检测花费的时间会很长的，针对于单个的测试目标的话，我们倒是可以全部选中这些攻击脚本，而如果我们是针对一批目标要检测的话，我还是建议选择特定的攻击脚本来进行扫描，图9。

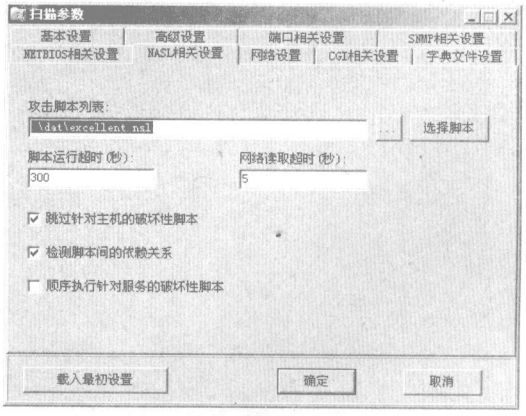

图8

图9

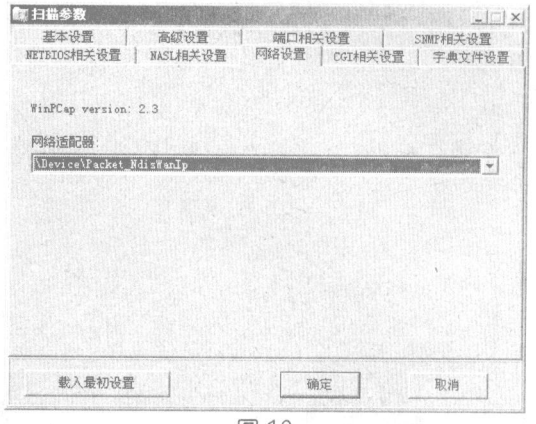

图10

在“网络设置”菜单中，我们可以看到x-scan3.1自带的的WinPCap 2.3，而网络适配器使用默认的就可以了，见图10。

“CGI相关设置”同早期的2.3版本中的差不多，使用默认的“HEAD”就可以了，你也可以根据需要选择别的方式，见图11。

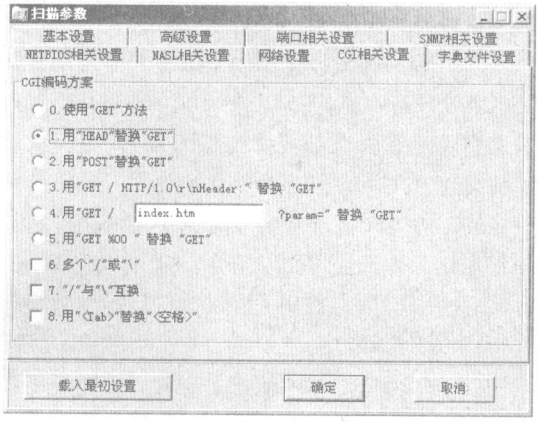

图11

“字典文件设置”中主要是x-scan3.1默认使用的的一些用于猜解远程帐号所用的字典文件，这些字典文件使用的大多是一些系统默认帐号，如果我们感觉这些字典文件的成功率太低的话，也可以手工打开这些文件来进行修改，不过，字典文件越大，用于猜解的时间也会越长，见图12。

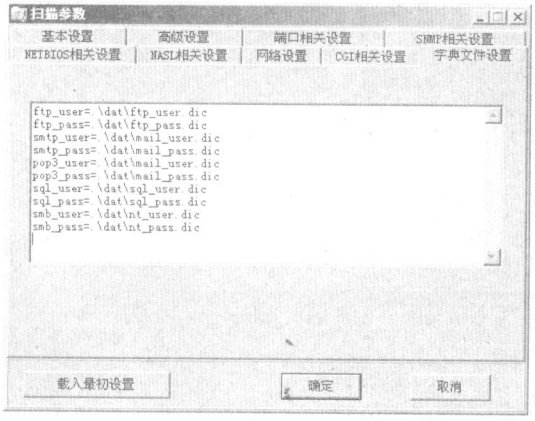

图12

设置好“扫描参数”后，我们打开“扫描模块”菜单，对于远程主机的检测主要有开放服务也就是开放端口情况、FTP的匿名登录、系统的弱口令、IIS编码/解码漏洞、CGI漏洞及Nessus攻击脚本等等。按照我们的需要来选择要检测的项目或是全部的项目，见图13。