

黑客兵器谱II

121个hack小工具教程+入档武器库推荐+工具探索手账

¥ 22.00 (电子书)



《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, 7期, 9期, 10期, 11期, 12期

单价: 8-8元

2004年——1期, 2期, 3期, 4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。为节省开支一律挂号邮寄, 请加寄挂号费3.00元。建议加挂号。

他们是独特的，他们的动力来源
于他们对技术的狂热兴趣，
他们执着于技术，追求技术永远是黑
客的第一目标，他们追求自由，寻求
在虚拟信息世界更大的生存空间和更
高的权限，他们提倡开放，致力于信
息高度共享。计算机和网络是他们的
生命。他们善于独立思考，喜欢自由
探索，要求破除一切霸权和枷锁，他
们痴迷与技术而不谙世俗常规，想法
狂热、新奇，有着强烈的好奇心，对
世界、社会、互联网的理解怪异，他
们对问题喜欢「打破沙锅问到底」，喜
欢「迎难而上」，喜欢挖掘自己的潜
力，他们不仅是技术高手，还往往呈
工作狂，为了解决一个技术难题常常
可以不吃不睡地连续工作好几十个
小时。正是有了这种精神特征，黑客才
不断地在互联网上制造神话，
这些神话其实靠的也是一百分的



Hacker X Files

不让生活磨灭我们的个性

自由 平等 随意 突破



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 果呆虫 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）

申明：本书所载文字及图片，版权所有，未经许可，不得转载。文章内容仅代表作者观点，与本书立场无关。投稿于本书的文章，均视为作者已授权本书合作媒体的使用。我们支付的稿费已包含了授权相关资费。如有相关问题，请作者及时与我们联系。

此为试读，需要完整PDF请访问：www.ortongbook.com

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，我们建议你详细的阅读本书，学习各种网络安全工具的应用，而如果你自诩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】

1.1 x-scan3.1 12

这是 x-scan 的最新版本, 功能比以前的版本提高了许多, 而且其 nasl 插件, 我感觉更是类似于 unix/linux 系统下的 nessus 扫描程序

1.2 流光 5 15

国内最优秀的综合网络安全检测(扫描)工具, 集安全检测、扫描、攻击于一身, 甚至在流光的目录下还收集了几个针对 unix/linux 系统的常用的远程溢出程序

1.3 x-way2.6 21

国内另一款不错的综合网络安全扫描工具, 也是集成了许多实用的小工具

1.4 nmap 25

unix/linux 下强大的端口检测程序, 这个是 windows 版本

1.5 SuperScann3 30

基于 windows 系统平台的使用最广泛的端口扫描程序, 速度快, 扫描的端口可自己根据需要随意的添加、选择。

1.6 ASC.exe 31

这是国内公布的一款用于扫描 ASP 文件是否存在注入点, 也就是是否存在脚本注入漏洞的工具

1.7 Sleuth1.4 32

非常不错的一款网页文件检查工具, 可检查的文件类型包括 php、pl、asp、htm、cfm、jsp、cgi、dll、txt

二、远程控制

【秘密潜入】

2.1 vnc 35

大名鼎鼎的远程控制软件, 最早使用于远程控制

unix/linux 系统, 不过, 也有 windows 版本

2.2 DameWare 37

基于 windows 系统平台的, 一款常用的远程控制软件

三、远程溢出

【刺穿你的防线】

3.1 sql2.exe 40

ms-sql 的远程溢出工具

3.2 thcsql.exe 41

ms-sql 的远程溢出工具

3.3 ispc 43

unicode 漏洞的利用工具

3.4 lis5hack 及 idahack 44

.printer 漏洞远程溢出工具

3.5 snake IIS 45

Snake ida、idq 的远程溢出工具

3.6 aspcode.exe 48

asp 漏洞远程溢出工具

3.7 webdavx3 49

webadv 漏洞远程溢出工具(isno)

3.8 webdav.exe 49

webdav 漏洞溢出工具(yuange)

3.9 rpc_locator.exe 及 rpc.exe 51

RPC LOCATOR 漏洞远程溢出工具

3.10 media.exe 55

media server 远程溢出工具

3.11 winrpcdcom.exe 56

windows rpcdcom 的远程溢出工具	
3.12 w2krpcdcom.exe	58
windows rpcdcom 远程溢出工具 (反向连接)	
3.13 rpcloname	59
windows rpcdcom 长文件名的远程溢出程序	
3.14 realex.exe	60
real server 的远程溢出工具, 支持 linux 系统及 windows 系统	
3.15 msghack.exe	62
windows messenger 漏洞的远程溢出程序(ms03-43)	
3.16 ms03049.exe	65
windows workstation 漏洞的远程溢出程序(ms03-049)	
3.17 winfp30reg2.exe	66
windows frontpage fp30reg.dll 的远程溢出程序 (ms03-051)	
3.18 ms04011lsass.exe	68
windows Lsassrv.dll RPC 远程溢出程序(ms04-011)	
3.19 winsslV02AutoHacker	70
windows SSL 漏洞的自动攻击程序(ms04-011)	
3.20 dameware.exe	72
dameware 的远程溢出工具	
3.21 serv345.exe	74
windows serv_u ftp 的远程溢出工具	
3.22 sun.exe	75
SUNOS telnet 远程溢出程序	
3.23 irixtelnet.exe	77
SGI IRIX telnet 远程溢出程序	

3.24 0x333samba.exe	78
Linux SAMBA 服务的远程溢出程序	
3.25 xservu.exe	79
windows servu ftp 5.0.0.4 的远程溢出工具	

四、入侵辅助

【无声配角】

4.1 NC(NetCat)	82
全能的“瑞士军刀”	
4.2 SqlInj.exe	84
脚本注入自动攻击程序	
4.3 mport	85
列举出打开端口的文件的一个工具	
4.4 AProMan.exe	86
查看系统进程的一个程序	
4.5 gina.exe	87
记录系统登录密码	
4.6 NTSHELLGINA.DLL	88
一个在图形界面下记录登录密码的工具	
4.7 klogger.exe	89
windows 系统下的一个键盘记录工具	
4.8 sqlexec.exe	90
windows ms-sql 数据库的连接程序	
4.9 tftpd32.exe	91
建立一个 tftp 服务器的工具	
4.10 whoami	92
查看当前用户名称的一个程序	
4.11 elseave	96

小榕推出的一个用于远程清除日志文件的工具

4.12 cleanislog 97

小榕推出的一个用于本地执行清除日志的工具

4.13 ERunasx 98

DEBUG 漏洞的本地溢出 (权限提升) 工具

4.14 winwmiex 99

wmi server 的本地溢出 (权限提升) 工具

4.15 xdebug 101

windows kernel 本地溢出 (权限提升) 工具

4.16 ptsec 103

windows 进程的本地溢出 (权限提升) 工具

4.17 local04011ex 104

MS 04-011 漏洞的本地溢出工具

4.18 T-SysCmd-1.0 106

win2000/xp 下提升权限的工具, 也可以当作一个后门程序来使用

五、后门

【寂寞的潜伏】

5.1 BITS 109

小榕推出的一款功能强大的 DLL 后门程序

5.2 PortlessNew 111

同小榕的 bits 类似的一个强大的后门程序

5.3 WinShell 114

一个小巧的后门程序

5.4 opentelnet 115

远程开启 windows telnet 服务的工具

5.5 Remoxec 116

不依赖 IPC 管道连接, 实现远程执行命令

5.6 GUIControlTelnet 118

图形界面下的远程开启、关闭 telnet 服务的工具

5.7 dtx3389.bat 119

远程开启目标主机的终端服务 (3389)

5.8 cmdasp.asp 120

最早的 asp 后门程序

5.9 ca.exe 121

小榕发布的一个用于克隆系统帐号的工具

5.10 ntlm.exe 124

清除 ntlm 认证的一个工具

5.11 nodoom 125

mydoom 病毒后门的利用程序

5.12 sasserftp 126

sasser 振荡波病毒的利用程序

5.13 superdoor3.0 128

windows 系统下一个隐藏帐号的工具

5.14 hxdef100 129

优秀的后门程序黑客守卫者

5.15 icmpdoor 132

WindowsNT/2000/xp 下的一个很好的 icmp 后门

5.16 icmd 134

Windows 下一个很小巧的后门工具

六、嗅探

【你的秘密我知道】

6.1 T-Sniffer 137

是一个基于 Windows 系统平台的图形界面的嗅探工具

6.2 winsniff 138

是一个基于命令行方式下的嗅探工具

6.3 xsniff 139

是安全焦点推出的 x-tools 系列中的一个 sniff (嗅探) 工具

6.4 xport 144

这是安全焦点推出的 x-tools 系列中的端口扫描工具

6.5 xftp 146

这是安全焦点推出的 x-tools 系统中的一个 ftp 工具, 可以实现文件的上传与下载

【七、Hacker 百宝箱】

【武装到牙齿】

7.1 FPipe 149

一个著名的端口重定向工具

7.2 P2P 150

端口重定向工具

7.3 superagent 151

协议转发工具

7.4 PortMap 153

端口映射工具

7.5 trtool.exe 155

红客联盟发布的一款协议转发工具

7.6 July 156

查看进程及进程中模块的一个工具

7.7 antiports 157

查看进程及使用的端口的一个工具

7.8 newletmein 158

一个用于获取系统用户列表信息的工具

7.9 portqryv2 160

微软发布的一款用于查看本地网络连接及远程主机开放端口信息的一个程序

7.10 Microsoft Baseline Security Analyzer 161

微软发布的一款系统安全检测工具

7.11 PEiD 163

一个非常著名的专门用于检测程序所加的壳的种类的工具

7.12 pe-scan 164

一款用于检测壳的种类以及脱壳的程序, 可以检测出壳的入口点、偏移量及 pep

7.13 ASProtect 166

一个非常不错的加壳的程序

7.14 unpacker upx 167

专门用于脱 UPX 壳的程序

7.15 PwDump3 168

windows 系统平台下一个著名的用于本地或远程获取系统密码散列的工具

7.16 LC4 169

windows 系统平台下最著名的一款用于破解系统帐号密码的工具

7.17 blades 1.25 171

小榕的乱刀, 专门用于破解 unix/linux 系统的帐号口令

7.18 John 175

unix/linux 下最著名的系统帐号破解工具了, 这个是 windows 系统下的版本

7.19 BrutusAET2 177

远程猜解口令的工具

7.20 tscrack-beta9 179

远程猜解 windows 终端服务 (3389) 口令的一个工具

7.21 Base64 180

base64 密码转换工具

7.22 jmpesp 180

sunx 编写的一个用于寻找 JMPESP、JMPEBX 地址的工具

7.23 sac 182

红客联盟发布的一个用于寻找 JMPESP、JMPEBX 地址的工具

7.24 提取 shellcode 的三个程序 183

提取 SHELLCODE 的三个程序: bindshellcode.exe、cbackshellcode.exe、downshellcode.exe

7.25 PuTTY 184

一个终端连接程序, 支持 telnet、SSH、rlogin

7.26 pstools 186

pstools 是一个集合了十二个实用小程序的工具集合了, 别小看了这十二个小工具, 可是非常实用的哟

psexec

psfile

psgetsid

psinfo

pskill

pslist

psloggedon

psloglist

pspasswd

pservice

psshutdown

pssuspend

7.27 winnuke 190

针对 windows 的 135 端口的一个拒绝服务 (D.O.S)

攻击程序

7.28 ms04007dos.exe 191

针对 windows ASN.1 漏洞(ms 04-007)的一个拒绝服务 (D.O.S) 攻击程序

7.29 独裁者 DDoS 攻击器 192

一个分布式拒绝服务(D.D.O.S)攻击程序

7.30 ldapbrowser253 194

LDAP 服务的远程连接管理程序(389 端口)

7.31 天网防火墙 2.51 的简单设置 .. 197

国内一款最常用的个人防火墙系统

7.32 IPF 200

一个基于命令行方式下的防火墙

7.33 winHex 的安装 202

windows 下的十六进制查看工具

7.34 W32Dasm 的简单使用 203

将程序转换为 ASM 的一个程序, 用于分析程序

7.35 ActivePerl 的安装 204

activeperl 是 windows 系统下最常使用的 perl 语言解释工具, 安装了它, 我们就可以在 windows 系统下正常的使用那些 perl 程序了

7.36 perl2exe 的简单使用 206

perl2exe 是常用的一款专门将 perl 程序转换成 exe 程序的工具, 这样, 转换后的程序不需要 activeperl, 也可以正常运行了

7.37 Cygwin 的安装 207

cygwin 是一个基于 windows 系统平台的 unix 环境模拟工具, 在 cygwin 下我们可以编译许多基于 gcc 的源代码, 以使这些程序能够运行在 windows 平台下





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。

rpclcname: Rpcdcom 长文件名的远程溢出。

realex.exe Real server 的远程溢出。

msgshack.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 Lsassrv.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。

SqliInj.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 察看当前用户名等。

erunasx DEBUG 漏洞的本地溢出。

winwmlex 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,并且它能利用 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 分区区的软件。

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。

linuextelnet 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。

winimail.exe Imail 的远程溢出程序。

winisspam Windows ISSPAM 远程溢出程序。

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

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

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。

第一章

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-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”。

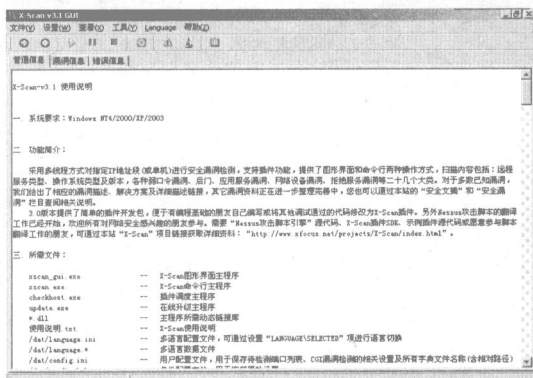


图 2

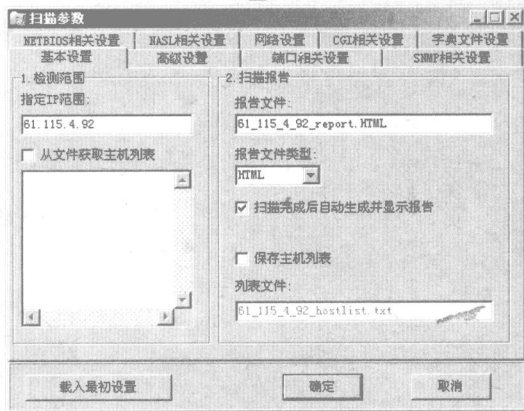


图 3

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详细的检测, 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”。

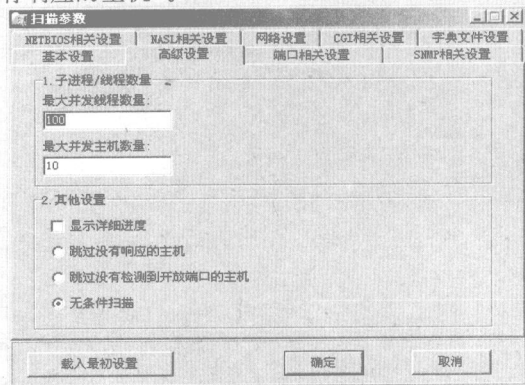


图4

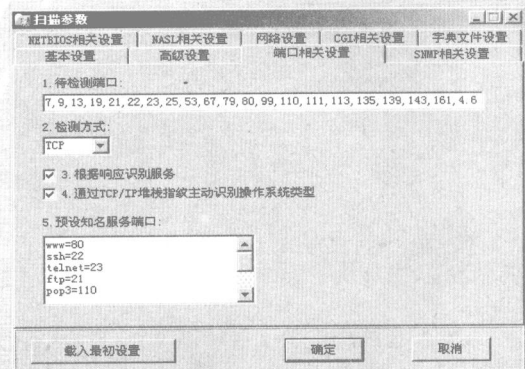


图5

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。

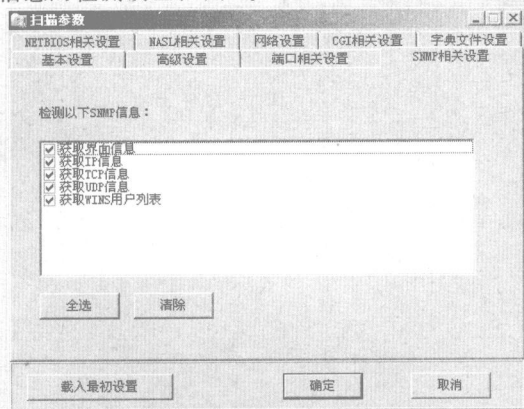


图6

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。

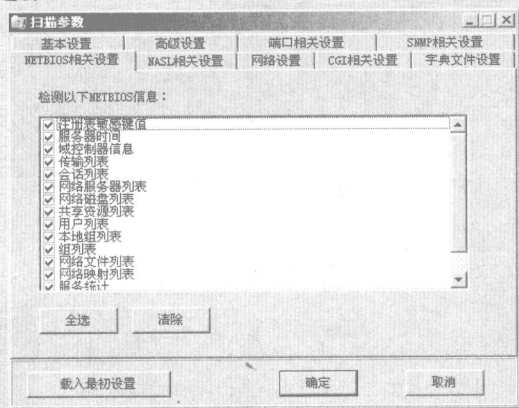
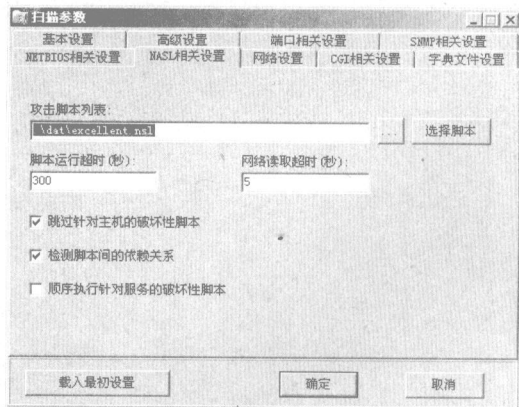


图7

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, 因此你可以根据需要进行选择, 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。



88 图

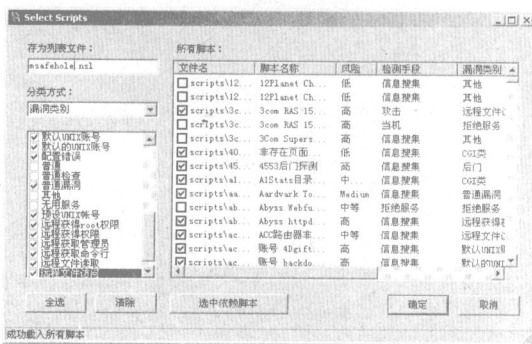


图 9

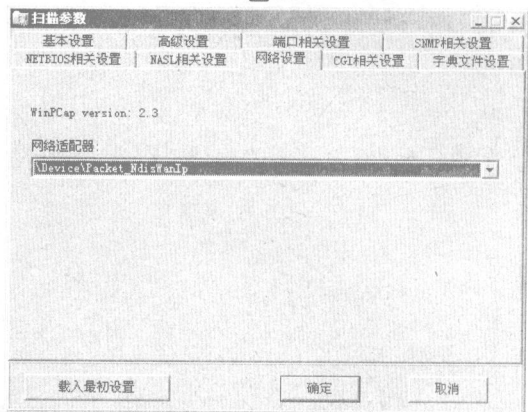


图 10

scan3.1 自带的 WinPCap 2.3, 而网络适配器使用默认就可以了, 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。

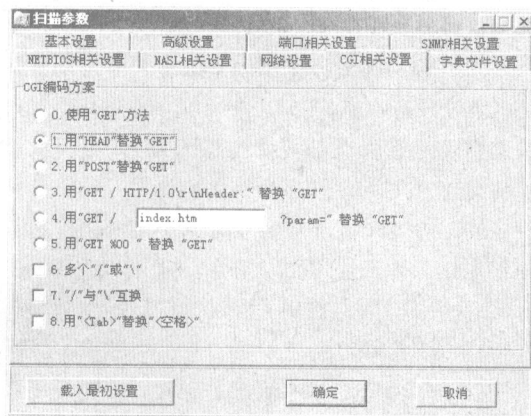


图 11

“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。

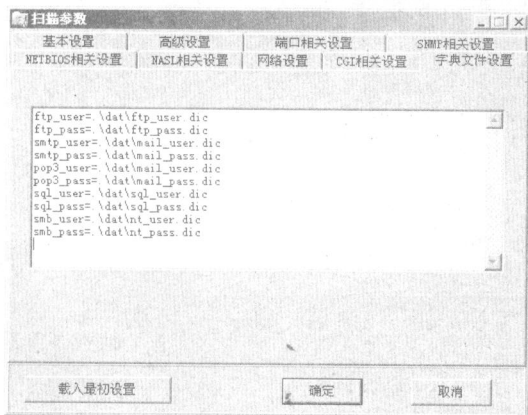


图 12

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。

在“网络设置”菜单中，我们可以看到 x-