电脑迷 荣誉出品

HEIKE RUMEN

黑客入门大曝光

黄建云 胡旻 编著

披露黑客练功全过程
识破黑客入侵小伎俩

山东电子音像出版社出版

黑客入门大曝光

HEIKE RUMEN

黄建云 胡旻 编著

披露黑客练功全过程
识破黑客入侵小伎俩

山东电子音像出版社出版

光盘导读

特别说明：本光盘提供的黑客软件仅供研究使用，切勿利用来破坏他人的计算机或数据，否则一切后果自负！

本光盘已经过严格杀毒，但因收录有黑客程序，所以在运行光盘时，某些杀毒软件可能会报警。

● 黑客必备软件

局域网工具\黑客必备软件\局域网工具

收集整理多个局域网小工具，包括guest删除大师、局域网共享破解软件和扫描局域网计算机工具等。

木马制作\黑客必备软件\木马制作

木马的危害极大，但是现在的木马杀灭技术也很高。要做到完全免杀，很难，这里提供了一些经典好用的木马免杀工具，希望你能喜欢。

破解类\黑客必备软件\破解类

最新破解软件、免费汉化破解软件大集合。

嗅探扫描软件\黑客必备软件\破解类

最受黑客欢迎的扫描、嗅探软件，能实现秘密扫描、动态延迟、重发与平行扫描、欺骗扫描、端口过滤探测、RPC直接扫描等。

远程攻击\黑客必备软件\破解类

这部分软件能实现远程攻击黑客还无法控制的计算机。

● 黑客经典视频

漏洞入侵

ipc攻击演示
sql2入侵实例
unicode生成视频
超级入侵(各种服务开启)
独裁者DDOS使用教程
通过Serv-u入侵
突破防火墙进入主机

网吧攻击

Pubwin 2007冲钱
Oo坏小子突破网吧新的限制
暴力破解QQ密码
简单突破QQ好友拒加，和MM聊天
教学教程ASP盗Q收信
快速查出盗号者
双重盗取QQ密码

木马入侵

改入口点和加多层壳打到木马表面内存免杀
灰鸽子内网FTP上线加配置最新服务端
利用BT狂扫肉鸡，服务端加牛X的免杀壳
利用影音文件连接挂马
全套挂马视频
图片木马制作
网马的详细制作加另类免杀 1
网马的详细制作加另类免杀 2
制作破SP2系统网马

破解类

获取ADSL帐号和密码
使用x-way进行邮箱密码破解
用cmd破解IPC口令

目 录

一、黑客必备知识和技能

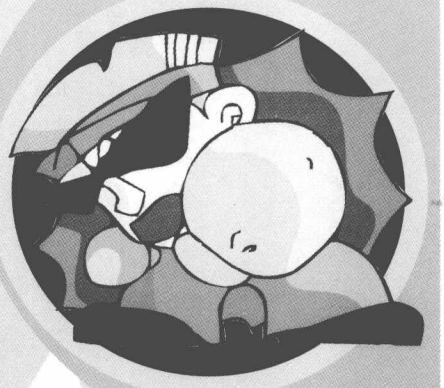
试读结束：需要全本请在线购买： www.ertongbook.com

四、黑客网吧攻防

五、无线网络的攻击

黑客

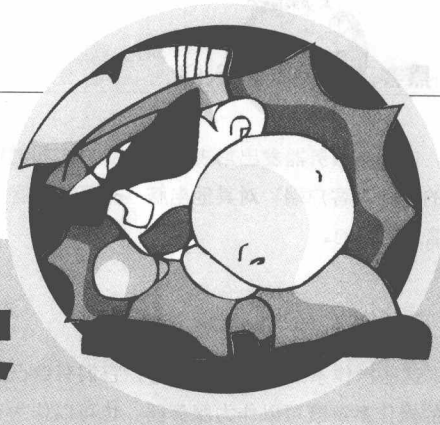
必备知识和技能



acker

heikebibeizhishihejineng

heikebibeizhishihejineng
heikebibeizhishihejinenghei
kebibeizhishihejinengheikebibeizhishihejinengheikebibeizhishihejinengheikebibeizhis
hihejinengheikebibeizhishihejinengheikebibeizhishihejinengheikebibeizhishihejineng



黑客必备知识和技能

随着Internet网络在国内的普及，跟随而来的各种黑客攻击的网络破坏行为接踵而来。我们要更好地防护，就必须了解黑客攻击的各种手法，掌握黑客的心理，所谓“知己知彼，百战不殆”。本章主要介绍初级黑客必须掌握的网络知识以及必备的黑客技能。

黑客需要知道的网络知识

网络协议

网络是一个信息交换的场所，所有接入网络的计算机都可以通过彼此之间的物理连接设备进行信息交换，这种物理设备包括最常见的电缆、光缆、无线WAP和微波等，但是单纯拥有这些物理设备并不能实现信息的交换，这就好像人类的身体不能缺少大脑的支配一样，信息交换还要具备软件环境，这种“软件环境”是人们规定好的一些规则，被称作“协议”，有了协议，不同的电脑可以遵照相同的协议使用物理设备，并且不会造成相互之间的“不理解”。

这种协议类似于“摩尔斯电码”，简单的一点一横，经过排列可以有万般变化，但是假如没有“对照表”，谁也无法理解一份杂乱无章的电码所表述的内容是什么。电脑也是一样，它们通过各种预先规定的协议完成不同的使命，例如RFC1459协议可以实现IRC服务器与客户端电脑的通信。因此无论是黑客还是网络管理员，都必须通过学习协议达到了解网络运作机理的目的。

每一个协议都是经过多年修改延续使用至今的，新产生的协议也大多是在基层协议基础上建立的，因而协议相对来说具有较高的安全机制，黑客很难发现协议中存在的安全问题从而直接入手进行网络攻击。但是对于某些新型协议，因为出现时间短、考虑欠周到，也可能会因安全问题而被黑客利用。

对于网络协议的讨论，更多人则认为：现今使用的基层协议在设计之初就存在安全隐患，因而无论网络进行什么样的改动，只要现今这种网络体系不进行根本变革，就无法从根本上杜绝网络黑客的出现。但是这种黑客机能已经超出了本书的范围，因而不在这里详细介绍。

服务器与客户端

最简单的网络服务形式是：若干台电脑作为客户端，使用一台电脑当作服务器，每一个客户端都具有向服务器提出请求的能力，而后由服务器应答并完成请求的动作，最后服务器会将执行结果返回给客户端电脑。这样的协议很多。例如我们平时接触的电子邮件服务器、网站服务器、聊天室服务器等都属于这种类型。另外还有一种连接方式，它不需要服务器的支持，而是直接将两个客户端电脑进行连接，也就是说每一台电脑都既是服务器又是客户端，它们之间具有相同的功能，对等地完成连接和信息交换工作。例如DCC传输协议即属于此种类型。

由此看出，客户端和服务器分别是各种协议中规定的请求申请电脑和应答电脑。作为一般的上网用户，

都是操作着自己的电脑（客户端），向网络服务器发出常规请求以完成诸如浏览网页、收发电子邮件等动作的，而对于黑客来说则是通过自己的电脑（客户端）对其他电脑（有可能是客户端，也有可能是服务器）进行攻击，以达到入侵、破坏、窃取信息的目的。

系统与系统环境

电脑要运作必须安装操作系统，这些操作系统各自独立运行，它们有自己的文件管理、内存管理、进程管理等机制，在网络上，这些不同的操作系统既可以作为服务器、也可以作为客户端被使用者操作，它们之间通过“协议”来完成信息的交换工作。

不同的操作系统配合不同的应用程序就构成了系统环境，例如Linux系统配合Apache软件可以将电脑构设成一台网站服务器，其他使用客户端的电脑可以使用浏览器来获得网站服务器上供浏览者阅读的文本信息；再如Windows2000配合FTPD软件可以将电脑构设成一台文件服务器，通过远程FTP登录可以获得系统上的各种文件资源等。

IP地址和端口

我们上网，可能会同时浏览网页、收发电子邮件、进行语音聊天……如此多的网络服务项目，都是通过不同的协议完成的，然而网络如此之大，我们的电脑怎么能够找到服务项目所需要的电脑？如何在一台电脑上同时完成如此多的工作的呢？这里就要介绍到IP地址了。

每一台上网的电脑都具有独一无二的IP地址，这个地址类似于生活中人们的家庭地址，通过网络路由器等多种物理设备，网络可以完成从一个电脑到另一个电脑之间的信息交换工作，因为它们的IP地址不同，所以不会出现找不到目标的混乱局面。但是黑客可以通过特殊的方法伪造自己电脑的IP地址，这样当服务器接受到黑客电脑（伪IP地址）的请求后，服务器会将应答信息传送到伪IP地址上，从而造成网络的混乱。当然，黑客也可以根据IP地址轻易的找到任何上网者或服务器，进而对他们进行攻击。

一台电脑上为什么能同时使用多种网络服务？这好像古时候一个城有几个城门一样，不同的协议体现在不同的网络服务上，而不同的网络服务则会在客户端电脑上开辟不同的端口（城门）来完成它的信息传送工作。当然，如果一台网络服务器同时开放了多种网络服务，那么它也要开放多个不同的端口（城门）来接纳不同的客户端请求。

网络上经常听到的“后门”就是这个意思，黑客通过特殊机能在服务器上开辟了一个网络服务，这个服务可以用来专门完成黑客的目的，那么服务器上就会被打开一个新的端口来完成这种服务，这个端口是供黑客使用的，因而不会被一般上网用户和网络管理员发现，即“隐藏的端口”。

每一台电脑都可以打开65535个端口，因而理论上可以开发出至少65535种不同的网络服务，但是网络应用中经常用到的服务协议不过几十个，例如浏览网页客户端和服务端都使用的是80号端口，进行IRC聊天则在服务端使用6667端口，客户端使用1026端口等。

系统漏洞

漏洞就是程序中没有考虑到的情况，例如最简单的“弱口令”漏洞是指系统管理员忘记屏蔽某些网络应用程序中的账号；Perl程序漏洞则可能是由于程序员在设计程序的时候考虑情况不完善而出现的“让程序执行起来不知所措”的代码段，“溢出”漏洞则属于当初设计系统或者程序的时候，没有预先保留出足够的资源，而在日后使用程序时造成的资源不足；特殊IP包炸弹实际上是程序在分析某些特殊数据的时候出现错误等。

试读结束：需要全本请在线购买：www.ertongbook.com

总而言之，漏洞就是程序设计上的人为疏忽，这在任何程序中都无法绝对避免，黑客也正是利用种种漏洞对网络进行攻击的。黑客利用漏洞完成各种攻击是最终的结果。

加密与解密

网络上最常使用的是设置个人密码和使用DES加密锁这两种加密方式，它们分别可以完成用户登录系统、网站、电子邮件信箱和保护信息包的工作，而黑客所要进行的工作，就是通过漏洞、暴力猜测、加密算法反向应用等方式获得加密档案的明文，有人把“魔高一尺，道高一丈”用在这里，的确是再恰当不过了！网络上的加密方法和需要验证密码的系统层出不穷，黑客也在寻找破解这些系统的种种办法。

可以说，“漏洞”和“解密”是两个完全不同的黑客领域，不同的学习者对它们的偏好，直接影响到今后他们将会成为什么样的黑客。

特洛伊木马

特洛伊木马是一个程序，这个程序可以做程序设计者有意设计的未出现过的事情。但是对于特洛伊木马所做的操作，不论是否用户了解，都是不被赞同的。根据某些人的认识，病毒是特洛伊木马的一个特例，即：能够传播到其他的程序当中（也就是将这些程序也变成特洛伊木马）。根据另外的人的理解，不是有意造成任何损坏的病毒不是特洛伊木马。最终，不论如何定义，许多人仅仅用“特洛伊木马”来形容不能复制的带有恶意的程序，以便将特洛伊木马与病毒区分开。

黑客不能不知道的命令

这里我们详细给出以下几个Windows系统自带的网络方面的命令，同时，这些命令也是作为一个菜鸟所必须掌握的，只有熟练使用才会对信息收集和安全防御带来便利。

测试物理网络的命令

命令格式为：Ping 计算机名/IP

比如：ping 192.168.10.88 -t，参数-t是等待用户去中断测试。

查看DNS、IP、Mac等

①查看本机的信息

Windows 98系统使用winipcfg

Windows 2000以上系统使用Ipconfig/all

②查看远程服务器的DNS：NSLOOKUP

比如键入：

C:\>nslookup

结果显示：

Default Server: ns.home.com

Address: 202.99.160.68

>

然后可以在“>”后面输入server IP，修改你的DNS，比如：

>server 202.99.41.2；则将DNS改为了41.2

> pop.home.com

Server: ns.home.com

Address: 202.99.160.68

Non-authoritative answer:

Name: pop.home.com

Address: 202.99.160.212

网络信使命令

Net send 计算机名/IP|*(广播) 传送内容，注意不能跨网段。

net stop messenger 停止信使服务。

net start messenger 开始信使服务。

探测对方计算机名，所在的组、域及当前用户名

ping -a IP -t，只显示NetBIOS。

nbtstat -a 192.168.10.146显示全部。

显示端口信息

netstat -a 显示计算机当前所开放的所有端口。

netstat -s -e 比较详细地显示网络资料，包括TCP、UDP、ICMP和IP的统计等。

探测ARP绑定（动态和静态）列表

显示和修改“地址解析协议 (ARP)”缓存中的项目。ARP缓存中包含一个或多个表，它们用于存储IP地址及其经过解析的以太网或令牌环物理地址。计算机上安装的每一个以太网或令牌环网络适配器都有自己单独的表。如果在没有参数的情况下使用，则arp命令将显示帮助信息。

语法

arp [-a [InetAddr] [-N IfaceAddr> [-g [InetAddr] [-N IfaceAddr> [-d InetAddr [IfaceAddr> [-s InetAddr EtherAddr [IfaceAddr>

参数

-a [InetAddr] [-N IfaceAddr]

显示所有接口的当前ARP缓存表。要显示指定IP地址的ARP缓存项，则使用带有InetAddr 参数的arp -a，此处的InetAddr代表指定IP地址。要显示指定接口的ARP缓存表，则使用-N IfaceAddr参数，此处的IfaceAddr代表分配给指定接口的IP地址。-N参数区分大小写。

-g [InetAddr] [-N IfaceAddr]与-a相同。

-d InetAddr [IfaceAddr]

删除指定的IP地址项，此处的InetAddr代表IP地址。对于指定的接口，要删除表中的某项，则使用IfaceAddr参数，此处的IfaceAddr代表分配给该接口的IP地址。要删除所有项，请使用星号“*”通配符代替InetAddr。

-s InetAddr EtherAddr [IfaceAddr]

向ARP缓存添加可将IP地址InetAddr解析成物理地址EtherAddr的静态项。要向指定接口的表添加静态ARP缓存项，请使用IfaceAddr参数，此处的IfaceAddr代表分配给该接口的 IP 地址。

/?

在命令提示符处显示帮助。

注释

InetAddr和IfaceAddr 的IP地址用带圆点的十进制记数法表示。

物理地址 EtherAddr 由六个字节组成，这些字节用十六进制记数法表示并且用连字符隔开（比如，00-AA-00-4F-2A-9C）。

通过-s参数添加的项属于静态项，它们不会在ARP缓存中超时。如果终止TCP/IP 协议后再启动，这些项会被删除。要创建永久的静态ARP缓存项，请在批处理文件中使用适当的arp命令并通过“计划任务程序”在启动时运行该批处理文件。

只有当网际协议(TCP/IP)协议在 网络连接中安装为网络适配器属性的组件时，该命令才可用。

范例

要显示所有接口的ARP缓存表，可键入：

arp -a

对于指派的IP地址为10.0.0.99的接口，要显示其ARP缓存表，可键入：

arp -a -N 10.0.0.99

要添加将IP地址10.0.0.80解析成物理地址00-AA-00-4F-2A-9C的静态ARP缓存项，可键入：

arp -s 10.0.0.80 00-AA-00-4F-2A-9C

在代理服务器端捆绑IP和MAC地址

绑定IP与MAC：ARP -s ip mac

比如：

ARP -s 192.168.10.59 00-50-ff-6c-08-75

解除网卡的IP与MAC地址的绑定：arp -d mac ip

比如：

ARP -d 00-50-ff-6c-08-75 192.168.10.59

在网络邻居上隐藏你的计算机

net config server /hidden:yes 开启

net config server /hidden:no 则为关闭

net命令

① net view，显示当前工作组服务器列表

当不带选项使用本命令时，它就会显示当前域或网络上的计算机上的列表，如图1-1所示。

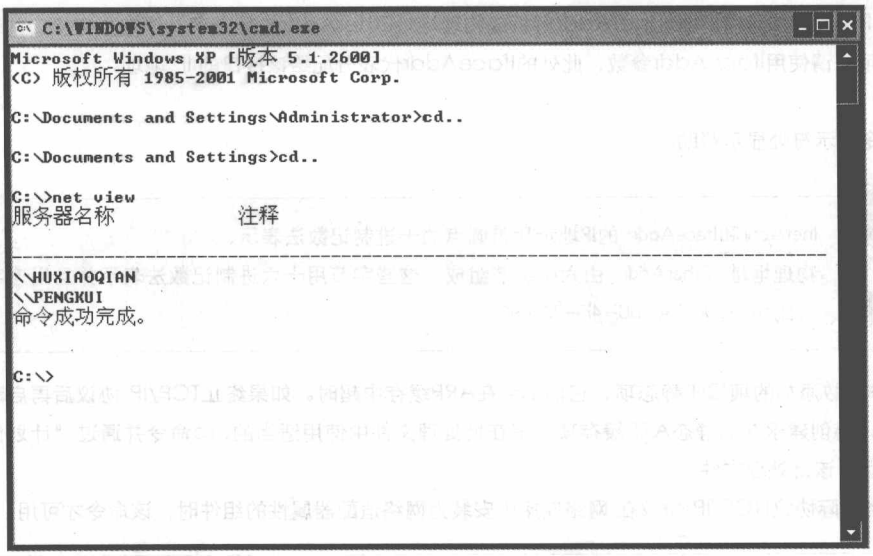


图1—1 net view

另外可以查看某个IP上的共享资源，如图 1-2所示。

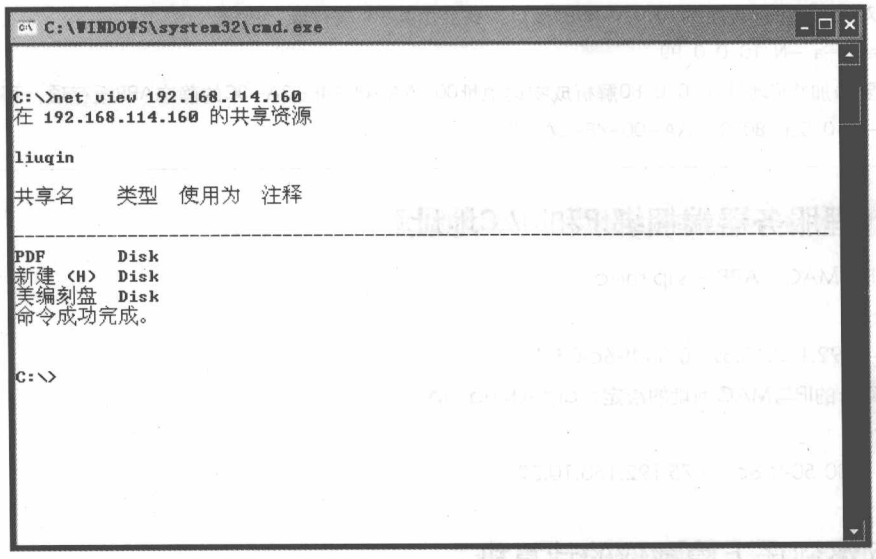


图1—2 查看某个IP上的共享资源

②net user，查看计算机上的用户账号列表

其命令和结果，如图1-3所示。

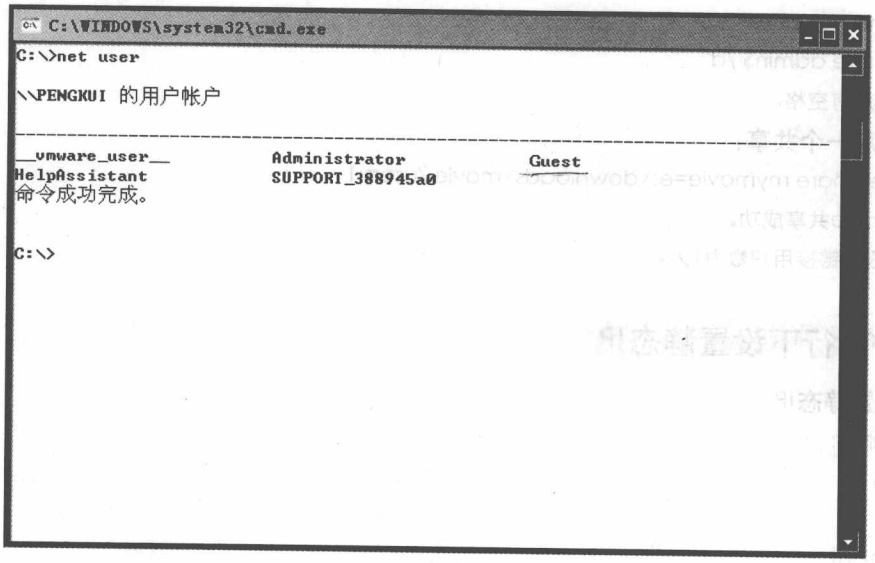


图1-3 查看账号列表

③net use，查看网络链接

例如：net use z: \\192.168.114.8\movie 将这个IP为192.168.114.8的电脑上的movie共享目录映射为本地的Z盘。

④net session，记录链接

例如：

C:\>net session

计算机 用户名 客户类型 打开空闲时间

\\192.168.10.110 ROME Windows 2000 00:03:12

\\192.168.10.51 ROME Windows 2000 00:00:39

命令成功完成。

路由跟踪命令

①tracert pop.home.com 显示路由信息

②pathping pop.home.com 除了显示路由外，还提供325S的分析，计算丢失包的百分率

共享安全的几个命令

①查看你机器的共享资源 net share

②手工删除共享

net share c$ /d

net share d$ /d

net share ipc$ /d

net share admin$ /d

注意$后有空格。

③增加一个共享：

c:\net share mymovie=e:\downloads\movie /users:1

mymovie共享成功。

同时限制链接用户数为1人。

在DOS行下设置静态IP

①设置静态IP

方式如下：

CMD

netsh

netsh>int

interface>ip

interface ip>set add “本地链接” static IP地址 mask gateway

②查看IP设置

在上面命令的部分基础上，再输入命令如下：

interface ip>show address

At命令

计划在指定时间和日期在计算机上运行命令和程序。at命令只能在“计划”服务运行时使用。如果在没有参数的情况下使用，则at列出已计划的命令。

语法

at [\\ComputerName] [{ID] [/delete] | /delete [/yes]}]

at <\\ComputerName] hours:minutes [/interactive] [{/every:date[,...] | /next:date[,...]}] command]

参数

\\computername

指定远程计算机。如果省略该参数，则at计划本地计算机上的命令和程序。

ID

指定指派给已计划命令的识别码。

/delete

取消已计划的命令。如果省略了ID，则计算机中所有已计划的命令将被取消。

/yes

删除已计划的事件时，对来自系统的所有询问都回答“是”。

hours:minutes

试读结束：需要全本请在线购买： www.ertongbook.com