一册在手 电脑金宝典 应用无忧

黑客入门与攻防精解

HEIKE RUMEN YU GONGFANG JINGJIE

赵磊◎主编

实用 权威 易懂

NEW 最新版

查找、锁定目标
开放端口及漏洞
直接入侵系统
寻找歼灭木马
……

远方出版社

实用 权威 易懂

一册在手 电脑金典 应用无忧

一册在手 应用无忧

YICE ZAISHOU YINGYONG WUYOU

黑客入门与攻防精解

赵磊⊙主编

NEW 最新版

远方出版社

图书在版编目(CIP)数据

黑客入门与攻防精解/赵磊主编. -呼和浩特:远方出版社,2009.7
(电脑金宝典)
ISBN 978-7-80723-435-7
Ⅰ.黑… Ⅱ.赵… Ⅲ.计算机网络-安全技术
Ⅳ.TP393.08
中国版本图书馆 CIP 数据核字(2009)第 115960 号

电脑金宝典

作　　者　赵　磊
责任编辑　刘卫伟
装帧设计　揽胜视觉
出版发行　远方出版社
社　　址　呼和浩特市乌兰察布东路 666 号
电　　话　0471-4919981(发行部)
邮　　编　010010
经　　销　全国新华书店
印　　刷　德富泰印务有限公司
开　　本　787 ×1092 毫米　1/16
字　　数　3000 千字
印　　张　225
版　　次　2009 年 9 月第 1 版
印　　次　2009 年 9 月第 1 次印刷
印　　数　3000 册
标准书号　ISBN 978-7-80723-435-7
定　　价　447.00 元(全 15 册)

前　言

为使您在最短时间内熟练的掌握电脑知识和操作技巧，为了满足广大电脑爱好者的需要，多年来我们研究不同层次的学习对象，总结了多位电脑高手和专家的经验，经数次修订和扩充，这套《电脑金宝典》系列丛书，终于出版面世了。

丛书特点

作为一套面向初、中级电脑用户的系列丛书，《电脑金宝典》的最大优势是合理的学习结构，简练流畅的语言，丰富实用的示例，以满足广大初学者的心愿。

丛书内容

本套丛书包括

《电脑组装自由做主》介绍了电脑选购、组装与维护的相关知识和操作技能。

《系统安装与重装完全掌握》全面的讲解了系统安装与重装的实际操作知识。

《电脑全能学技巧 6000 招》全面系统地介绍了使用电脑的常用方法与技巧。

《InDesign CS4 案例精解》全面、系统地讲述了 InDesign 的使用方法和技巧。

《Office 电脑办公一点通》以精练的语言和丰富的图例帮助初学者进行电脑办公的学习。

《五笔打字新手速成》全面系统地介绍了五笔字型输入法的基础知识和使用方法。

《Photoshop CS4 图像处理》介绍了 Photoshop CS4 各项基础操作和图像处理方面的功能。

《Windows 应用入门技巧》讲解了 Windows XP/Vista 两种系统的安装详解及基本操作。

《AutoCAD 2009 完全掌握》介绍了使用中文版 AutoCAD 2009 绘制工程图的方法和技巧。

《网管实战》介绍网络组建、设备选购、配置技巧、共享资源管理、服务器远程管理及网络安全管理等。

《黑客入门与攻防精解》讲解黑客入侵原理，重视网络安全，并采取相关措施现场自救。

《电脑入门操作新概念》本书将帮助您尽快认识电脑，为进一步学习电脑知识打下基础。

《电脑医生好秘方》介绍各种外设及操作系统等常用软件方面的故障实例。

《电脑故障急救 1000 招》主要帮助读者解决在日常使用电脑时所遇到的各种问题。

《新手上网一本通》本书主要解决新手上网时碰到的各种问题。

目 录

第6章 行踪隐藏与痕迹清理

第7章 QQ攻击大揭密

第8章 嗅探器截取数据与防范

第9章 邮件欺骗与轰炸

1 黑客基础知识

随着互联网技术的飞速发展，网络世界的安全性不断受到挑战。如果你要上网，就免不了遇到黑客的侵扰。本章就为大家介绍一些最基本的黑客入门知识，揭密黑客常用的一些命令，当然这些微不足道的伎俩难以入侵戒备森严的网络，不过至少让初学者对黑客的“工作情形”有初步的认识。

1.1 黑客简单介绍

最早的计算机于1946年在宾夕法尼亚大学出现，而最早的黑客出现于麻省理工学院(贝尔实验室也有)。最初的黑客一般都是一些高级的技术人员，他们热衷于挑战、崇尚自由并主张信息的共享。

1.1.1 黑客的历程

1994年以来，因特网在全球的迅猛发展为人们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，信息已成为物质和能量以外维持人类社会第三资源，它是未来生活中的重要介质。但是随着计算机的普及和因特网技术的迅速发展，黑客也随之出现了。

1.1.2 黑客的由来

“黑客”一词是由英语“Hacker”英译出来的，是指专门研究、发现计算机和网络漏洞的计算机爱好者，他们伴随着计算机和网络的发展而产生成长。黑客对计算机有着狂热的兴趣和执着的追求，他们不断地研究计算机和网络知识，发现计算机和网络中存在的漏洞，喜欢挑战高难度的网络系统并从中找到漏洞，然后向管理员提出解决和修补漏洞的方法。

黑客的出现推动了计算机和网络的发展与完善。他们所做的不是恶意破坏，他们是一群纵横于网络上的大侠，追求共享、免费，提倡自由、平等。黑客的存在是由于计算机技术的不健全，从某种意义上来讲，计算机的安全需要更多黑客去维护。这里我们借用黑客英雄网站长 myhk 的一句话：“黑客存在的意义就是使网络变得日益安全完善”。

但是到了今天，黑客一词已经被用于那些专门利用计算机进行破坏或入侵他人电脑的代言词，对这些人正确的叫法应该是Cracker，有人也翻译成“骇客”，也正是由于这些人的出现玷污了“黑客”一词，使人们把黑客和骇客混为一体，误认为黑客也是在网络上进行破坏的人。根据开放原始码计划创始人 EricRaymond(埃里克.雷蒙德)的解释，Hacker 与 Cracker 是分属两个不同世界的族群，基本差异在于，Hacker 是有建设性的，而 Cracker 则专门搞破坏。

1.2 黑客入侵流程

黑客在进行攻击时通常有个习惯性的流程。首先搜寻到目标信息系统，然后找到目标信息系统的弱点，并利用弱点获得权限开辟后门，最后对痕迹进行清除。

1.2.1 目标系统信息收集

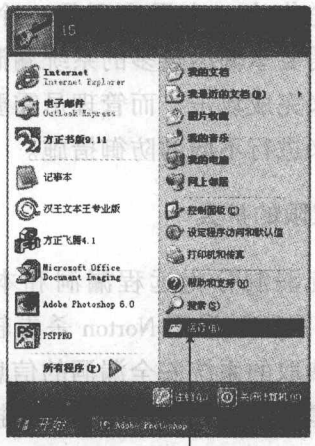
信息的收集并不对目标系统产生危害，只是为进一步的入侵提供有用信息。这些信息主要包括目标的操作系统类型及版本，目标主机提供哪些服务，各服务器程序的类型与版本以及相关的社会信息等。

要攻击一台机器，首先要确定它正在运行的操作系统版本。因为对于不同类型的操作系统，系统漏洞有很大区别，攻击的方法也完全不同，甚至同一种操作系统的不同版本的系统漏洞也是不一样的。要确定一台服务器的操作系统一般是靠经验，有些服务器

的某些服务显示信息会泄露其操作系统。

【案例 1-1】Telnet 登录 Linux 服务器示例

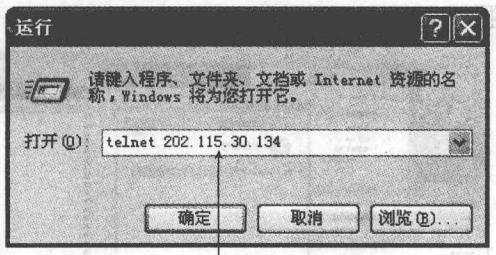
如果用户是在 Windows 的环境下，想对远程的 Linux 系统进行操作，推荐选择“telnet”的方式进行登录(telnet 命令在后有详细的介绍)，具体步骤如下。



Step 1 单击“运行”

Step 1

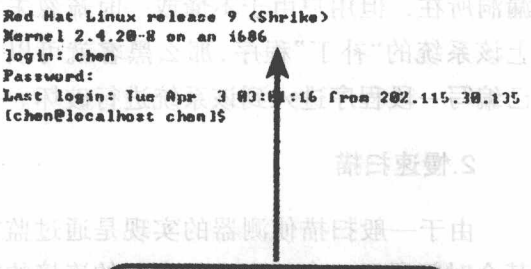
启动 Windows 操作系统，单击执行“开始”→“运行”命令。



Step 2 输入命令

Step 2

弹出的“运行”对话框中输入“telnet+远程 Linux 系统 IP 地址”，例如：telnel 202.115.30.134。



Step 3 登录结果

Step 3

弹出“RedHatLinux”界面，输入用户名和密码后，即可像在本机一样进行命令行的操作了，从图中可以得知该版本为 Red Hat Linux release 9 版本。

另外需要获得的信息就是一些与计算机本身没有关系的社会信息，例如网站所属公司的名称、规模，网络管理员的生活习惯、电话号码等。这些信息看起来与攻击一个网站没有关系，实际上很多黑客都是利用了这类信息攻破网站的。例如有些网站管理员用自己的电话号码做系统密码，这就很容易被人试探出来。

信息收集可以用手工进行，也可以利用工具来完成，完成信息收集的工具叫做扫描器。用扫描器收集信息的优点是速度快，可以一次对多个目标进行扫描。

1.2.2 弱点信息挖掘分析

在收集到一些准备要攻击目标的信息后，黑客们会探测目标网络上的每台主机，来寻求系统内部的安全漏洞，这些信息即所谓的弱点信息，主要探测的方式如下。

1.自编程序

对某些系统，互联网上已发布了其安全

漏洞所在，但用户由于不懂或一时疏忽未打上该系统的“补丁”程序，那么黑客就可以自己编写一段程序进入到该系统进行破坏。

2.慢速扫描

由于一般扫描侦测器的实现是通过监视某个时间段里一台特定主机发起的连接的数目来决定是否在被扫描，这样黑客可以通过使用扫描速度慢的扫描软件进行扫描。

3.体系结构探测

黑客利用一些特殊的数据包传送给目标主机，使其做出相对应的响应。由于每种操作系统的响应时间和方式都是不一样的，黑客利用这种特征把得到的结果与准备好的数据库中的资料相对照，从中便可轻而易举地判断出目标主机操作系统所用的版本及其他相关信息。

1.2.3 目标使用权限获取

1.获得权限

当收集到足够的信息之后，攻击者就要开始实施攻击行动了。作为破坏性攻击，只需利用工具发动攻击即可。而作为入侵性攻击，往往要利用收集到的信息，找到其系统漏洞，然后利用该漏洞获取一定的权限。有时获得了一般用户的权限就足以达到修改主页等目的了，但作为一次完整的攻击是要获得系统最高权限的，这不仅是为了达到一定的目的，更重要的是证明攻击者的能力，这也符合黑客的追求。

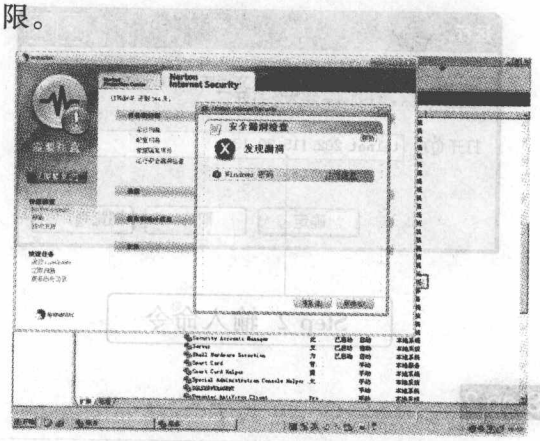
能够被攻击者所利用的漏洞不仅包括系统软件设计上的安全漏洞，也包括由于管理配置不当而造成的漏洞。

当然大多数攻击成功的范例还是利用了系统软件本身的漏洞。造成软件漏洞的主要原因在于编制该软件的程序员缺乏安全意识。当攻击者对软件进行非正常的调用请求时，会造成缓冲区溢出或者对文件的非法访问。其中利用缓冲区溢出的攻击最为普遍，据统计 80%以上成功的攻击都是利用了缓冲区溢出漏洞来获得非法权限的。

无论作为一个黑客还是一个网络管理员，都需要掌握尽量多的系统漏洞。黑客需要用它来完成攻击，而管理员需要根据不同的漏洞来进行不同的防御措施。

2.权限的扩大

系统漏洞分为远程漏洞和本地漏洞两种，如下图所示采用 Norton 杀毒软件漏洞扫描功能获取的系统安全漏洞的信息。远程漏洞是指黑客可以在别的机器上直接利用该漏洞进行攻击并获取一定的权限。这种漏洞的威胁性相当大，黑客的攻击一般都是从远程漏洞开始的。但是利用远程漏洞获取的不一定是最高权限，而往往只是一个普通用户的权限，这样常常没有办法做黑客们想要做的事。这时就需要配合本地漏洞来把获得的权限进行扩大，常常是扩大至系统的管理员权限。



只有获得了最高的管理员权限之后，才可以做诸如网络监听、打扫痕迹之类的事情。完成了权限的扩大后，不但可以利用已

获得的权限在系统上执行利用本地漏洞的程序，还可以放一些木马之类的欺骗程序来套取管理员密码，这种木马是放在本地套取最高权限用的，而不能进行远程控制。

1.2.4 开辟后门

黑客对目标主机进行了分析后，如果找到其弱点并打开了这台主机的后门，这时就可以向目标主机上传间谍程序了（通常黑客在目标主机上装上间谍程序后，会将 IPC$连接断开，不然在会话中将留有记录）。

通过后门上传的间谍程序可以是做代理的跳板程序，也可以是扫描程序，还可以是嗅探器，这些程序通常都隐藏得很深。例如目标主机没有嗅探器，黑客就可以为其安装上 Sniffer，用于监听 FTP/POP3 等的明文传输密码；如果目标主机开启了 Web 服务，那还可以给它安上一个脚本木马，脚本木马如果放得好的话，检测难度非常大，而管理员在做 Web 备份的时候，也会把它备份进去，一个好的 asp 木马可以完全接管一台 NT 操作系统。然后把主机上有用的文件全部下载下来，如 Web 程序的数据库连接代码里会有数据库用户名和口令信息，可以利用后面章节中所讲的对 MSSQL 的入侵来完全控制主机。

1.2.5 黑客常用手法

1.口令入侵

所谓口令入侵是指使用某些合法用户的账号和口令登录到目的主机，然后再实施攻击活动。这种方法的前提是必须先得到该主机上的某个合法用户的账号，然后再进行合法用户口令的破译。获得普通用户账号的方法很多，例如利用目标主机的 Finger 功能：当用 Finger 命令查询时，主机系统会将保存的用户资料（如用户名、登录时间等）显示在终端或计算机上；利用目标主机的 X.500 服务：有些主机没有关闭 X.500 的目录查询服务，也给攻击者提供了获得信息的一条简易途径；从电子邮件地址中收集：有些用户电子邮件地址常会透露其在目标主机上的账号；查看主机是否有习惯性的账号：有经验的用户都知道，很多系统会使用一些习惯性的账号，造成账号的泄露。

口令又有三种方法：

（1）通过网络监听非法得到用户口令，这类方法有一定的局限性，但危害性极大。监听者往往采用中途截击的方法也是获取用户账户和密码的一条有效途径。当下，很多协议根本就没有采用任何加密或身份认证技术，如在 Telnet、FTP、HTTP、SMTP 等传输协议中，用户账户和密码信息都是以明文格式传输的，此时若攻击者利用数据包截取工具便可很容易收集到你的账户和密码。还有一种中途截击攻击方法更为厉害，它可以在你同服务器端完成“三次握手”建立连接之后，在通信过程中扮演“第三者”的角色，假冒服务器身份欺骗你，再假冒你向服务器发出恶意请求，其造成的后果不堪设想。另外，攻击者有时还会利用软件和硬件工具时刻监视系统主机的工作，等待记录用户登录信息，从而取得用户密码；或者编制有缓冲区溢出错误的 SUID 程序来获得超级用户权限。

（2）在知道用户的账号后（如电子邮件 @ 前面的部分）利用一些专门软件强行破解用户口令，这种方法不受网段限制，但攻击者要有足够的耐心和时间。如：采用字典穷举法（或称暴力法）来破解用户的密码。攻击者可以通过一些工具程序，自动地从电脑字典中取出一个单词，作为用户的口令，再输入给远端的主机，申请进入系统；如果口令错

误，就按序取出下一个单词，进行下一个尝试，并一直循环下去，直到找到正确的口令或字典的单词试完为止。由于这个破译过程由计算机程序来自动完成，因而几个小时就可以把上十万条记录的字典里所有单词都尝试一遍。

（3）利用系统管理员的失误。在现代的Unix操作系统中，用户的基本信息存放在“password”文件中，而所有的口令则经过DES加密方法加密后专门存放在一个叫“shadow”的文件中。黑客们获取口令文件后，就会使用专门的破解DEs加密法的程序来解口令。同时，由于为数不少的操作系统都存在许多安全漏洞、Bug或一些其他设计缺陷，这些缺陷一旦被找出，黑客就可以长驱直入。

2.放置特洛伊木马程序

特洛伊木马程序可以直接侵入用户的电脑并进行破坏，它常被伪装成工具程序或者游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在用户的电脑中，并在用户的计算机系统中隐藏一个可以在Windows启动时悄悄执行的程序。当你连接到因特网上时，这个程序就会通知攻击者，报告你的IP地址以及预先设定的端口。攻击者在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改你的计算机的参数设定、复制文件、窥视你整个硬盘中的内容等，从而达到控制你的计算机的目的。

3.WWW的欺骗技术

在网上用户可以利用IE等浏览器进行各种各样的Web站点访问，如阅读新闻组、咨询产品价格、订阅报纸、电子商务等。然而一般的用户恐怕不会想到有这些问题存在：正在访问的网页已经被黑客篡改过，网页上的信息是虚假的！例如黑客要将用户要浏览的网页的URL改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的了。

一般Web欺骗使用两种技术手段，即URL地址重写技术和相关信息掩盖技术。利用URL地址，使这些地址都向攻击者的Web服务器，即攻击者可以将自己的Web地址加在所有URL地址的前面。这样，当用户与站点进行安全链接时，就会毫不防备地进入攻击者的范围，于是所有信息便处于攻击者的监视之中。但由于浏览器材一般均设有地址栏和状态栏，当浏览器与某个站点链接时，可以在地址栏和状态样中获得连接中的Web站点地址及其相关的传输信息，用户由此可以发现问题，所以攻击者往往在URL地址重写的同时，利用相关信息，即一般用JavaScript程序来重写地址，以达到欺骗的目的。

4.电子邮件攻击

电子邮件是互联网上运用得十分广泛的一种通讯方式。攻击者可以使用一些邮件炸弹软件或CGI程序向目的邮箱发送大量内容重复、无用的垃圾邮件，从而使目的邮箱被撑爆而无法使用。当垃圾邮件的发送流量特别大时，还有可能造成邮件系统对于正常的工作反映缓慢，甚至瘫痪。相对于其它的攻击手段来说，这种攻击方法具有简单、见效快等优点。

电子邮件攻击主要表现为两种方式：

（1）电子邮件轰炸和电子邮件“滚雪球”，也就是通常所说的邮件炸弹，指的是用伪造的IP地址和电子邮件地址向同一信箱发送

数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被“炸”，严重者可能会给电子邮件服务器操作系统带来危险，甚至瘫痪。

（2）电子邮件欺骗攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令（口令可能为指定字符串）或在看起来像正常的附件中加载病毒或其他木马程序。

5.通过一个节点来攻击其他节点

攻击者在突破一台主机后，往往以此主机作为根据地，攻击其他主机（以隐蔽其入侵路径，避免留下蛛丝马迹）。他们可以使用网络监听方法，尝试攻破同一网络内的其他主机；也可以通过 IP 欺骗和主机信任关系，攻击其他主机。

这类攻击很狡猾，但由于某些技术很难掌握，如 TCP/IP 欺骗攻击。攻击者通过外部计算机伪装成另一台合法机器来实现。它能破坏两台机器间通信链路上的数据，其伪装的目的在于哄骗网络中的其它机器误将其攻击者作为合法机器加以接受，诱使其它机器向他发送据或允许它修改数据。TCP/IP 欺骗可以发生 TCP/IP 系统的所有层次上，包括数据链路层、网络层、运输层及应用层均容易受到影响。如果底层受到损害，则应用层的所有协议都将处于危险之中。另外由于用户本身不直接与底层相互相交流，因而对底层的攻击更具有欺骗性。

6.网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。因为系统在进行密码校验时，用户输入的密码需要从用户端传送到服务器端，而攻击者就能在两端之间进行数据监听。此时若两台主机进行通信的信息没有加密，只要使用某些网络监听工具（如 NetXRay、Sniffit 等）就可轻而易举地截取包括口令和账号在内的信息资料。虽然网络监听获得的用户账号和口令具有一定的局限性，但监听者往往能够获得其所在网段的所有用户账号及口令。

7.利用黑客软件攻击

利用黑客软件攻击是互联网上比较多的一种攻击手法。BackOrifice2000、冰河等都是比较著名的特洛伊木马，它们可以非法地取得用户电脑的超级用户权限，可以对其进行完全的控制，除了可以进行文件操作外，同时也可以将对方桌面进行抓图、取得密码等操作。这些黑客软件分为服务器端和用户端，当黑客进行攻击时，会使用用户端程序登录上已安装好服务器端程序的电脑，这些服务器端程序都比较小，一般会随附带于某些软件上。有可能当用户下载了一个小游戏并运行时，黑客软件的服务器端就安装完成了，而且大部分黑客软件的重生能力比较强，给用户进行清除造成一定的麻烦。特别是最近出现了一种 TXT 文件欺骗手法，表面看上去是一个 TXT 文本文件，但实际上却是一个附带黑客程序的可执行程序，另外有些程序也会伪装成图片和其他格式的文件。

8.安全漏洞攻击

许多系统都有这样那样的安全漏洞（Bugs）。其中一些是操作系统或应用软件本身具有的，如缓冲区溢出攻击。由于很多系统在不检查程序与缓冲之间变化的情况，就任意接受任意长度的数据输入，把溢出的数据放在堆栈里，系统还照常执行命令。这样攻击者只要发送超出缓冲区所能处理的长度

的指令，系统便进入不稳定状态。若攻击者特别配置一串准备用作攻击的字符，他甚至可以访问根目录，从而拥有对整个网络的绝对控制权。另一些是利用协议漏洞进行攻击。如攻击者利用 POP3 一定要在根目录下运行的这一漏洞发动攻击，破坏根目录，从而获得超级用户的权限。又如，ICMP 协议也经常被用于发动拒绝服务攻击。它的具体手法就是向目的服务器发送大量的数据包，几乎占取该服务器所有的网络宽带，从而使其无法对正常的服务请求进行处理，而导致网站无法进入、网站响应速度大大降低或服务器瘫痪。现在常见的蠕虫病毒或与其同类的病毒都可以对服务器进行拒绝服务攻击的进攻。它们的繁殖能力极强，一般通过 Microsoft 的 Outlook 软件向众多邮箱发出带有病毒的邮件，而使邮件服务器无法承担如此庞大的数据处理量而瘫痪。对于个人上网用户而言，也有可能遭到大量数据包的攻击使其无法进行正常的网络操作。

9.端口扫描攻击

所谓端口扫描，就是利用 Socket 编程与目标主机的某些端口建立 TCP 连接、进行传输协议的验证等，从而侦知目标主机的扫描端口是否是处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等等。常用的扫描方式有：Connect 扫描。Fragmentation 扫描。

10.驱动攻击

当有些表面看来无害的数据被邮寄或复制到 Internet 主机上并被执行发起攻击时，就会发生数据驱动攻击。例如，一种数据驱动的攻击可以造成一台主机修改与安全相关的文件，从而使入侵者下一次更容易入侵该系统。

11.信息攻击

攻击者通过发送伪造的路由信息，构造源主机和目标主机的虚假路径，从而使流向目标主机的数据包均经过攻击者的主机。这样就给攻击者提供了敏感的信息和有用的密码。

12.系统管理员失误攻击

网络安全的重要因素之一就是人！无数事实表明“堡垒最容易从内部攻破”。因而人为的失误，如 WWW 服务器系统的配置差错，普通用户使用权限扩大等，就给黑客造成了可乘之机，黑客常利用系统管理员的失误，使攻击得到成功。

1.3 黑客常用命令

1.3.1 ping 命令

1.命令介绍

ping 是用来进行网络连接测试的一个程序，其对应的文件名为“ping.exe”（在WindowsXP系统下此文件存在于C:\Windows\System32文件夹下）。此工具的最简单的用法是：“ping XXX.XXX.XXX.XXX”（欲测试的IP地址），根据不同的测试目的可以带上不同的参数。使用ping可以测试计算机名和计算机的IP地址，验证与远程计算机的连接，通过将icmp回显数据包发送到计算机并侦听回复数据包来验证与一台或多台远程计算机的连接，此命令只有在安装了TCP/IP协议后才可以使用。

2.使用方式图解

ping命令的使用很简单，在命令控制行