黑骑士突出重围——

黑客攻防全攻略

陈芳 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

黑骑士突出重围

黑客攻防全攻略

陈芳 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书由浅入深地讲解了黑客攻击和防范的具体方法和技巧，通过具体形象的案例介绍向读者展示了多种攻击方法和攻击工具的使用。本书内容分为 14 章，分别介绍黑客攻防基础修炼，常见的黑客攻击方式，针对 IIS 服务器的漏洞攻防，网游黑客任我行，网络通信工具深度入侵，针对电子邮箱的攻击与防范，针对 IE 浏览器的恶意攻击与防范，Windows 操作系统的漏洞攻防解析，木马植入攻击和防范，注入攻防实战解析，扫描、嗅探和欺骗经典工具，以及病毒防范等内容。

本书以清晰明朗的思路，力求用图文并茂的形式，由浅入深地引导读者加强计算机安全意识。本书适合多个层次的网络爱好者阅读，也可以作为网络安全人员及网络管理员的参考书籍。

图书在版编目（CIP）数据

黑骑士突出重围：黑客攻防全攻略 / 陈芳编著. —北京：电子工业出版社，2007.12
ISBN 978-7-121-04963-7

Ⅰ. 黑… Ⅱ. 陈… 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（2007）第 135907 号

责任编辑：朱沭红
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　. 1/16　印张：25.5　字数：533 千字
印　　次：2007 年 12 月第 1 次印刷
印　　数：5000 册　定价：39.90 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

黑客（hacker），源于英语动词 hack，意为“劈，砍”，引申为“干了一件非常漂亮的工作”。在麻省理工学院早期的校园俚语中，“黑客”则有“恶作剧”之意，尤指手法巧妙、技术高明的恶作剧。在日本《新黑客词典》中，对黑客的定义是“喜欢探索软件程序奥秘，并从中增长其个人才干的人。他们不像绝大多数电脑使用者那样，只规规矩矩地了解别人指定了解的狭小部分知识。”由这些定义中，我们还看不出太多的贬义。黑客通常具有高级的硬件和软件知识，并有能力通过创新的方法剖析系统。他们能使更多的网络趋于完善和安全，他们以保护网络为目的，而以不正当入侵为手段来找出网络漏洞。

另一种入侵者是那些利用网络漏洞破坏网络的人，他们往往做一些重复的工作（如用暴力法破解口令）。他们也具备广泛的电脑知识，但与黑客不同的是他们以破坏为目的。这些群体称为“骇客”。当然还有一种人介于黑客与入侵者之间。

随着科学技术的发展以及网络的普及，越来越多的人开始投入到网络生活中来，然而人们在享受便利的网络生活的同时，还要时刻面临黑客们残酷攻击的危险，所以，应众多网民的要求，我们根据自己的亲身体验编写了此书。

本书由浅入深地讲解了黑客攻击和防范的具体方法和技巧，通过具体形象的案例介绍向读者展示了多种攻击方法和攻击工具的使用，按照由浅入深的方式，分为两大部分：第一部分是快速入门篇——黑骑士闭关修炼，主要讲述与黑客相关的基础知识和技巧；第二部分是实战篇——黑骑士驰骋沙场，介绍了黑客攻击的具体案例，分析各种黑客攻防的完整过程。

按照不同的黑客攻防内容，本书共分为 14 章。内容分别如下：

循序渐进

快速入门篇

- 黑客攻防基础修炼：介绍黑客攻防的原理和流程，以及一些常见的攻击工具，并通过使用 Syskey 双重加密实例讲述了黑客预防的具体措施。
- 黑客攻击的常用招式：介绍黑客攻击的常用方式，包括缓冲区溢出攻击、网络欺骗攻击、口令猜测攻击，以及恶意代码攻击等，并且在讲述攻击原理后带有攻防实例讲解。
- IIS 漏洞攻击的软肋：针对关于 IIS 服务器的漏洞，进行了攻防讲解，主要讲述了 Unicode 漏洞攻防和.printer 缓冲区漏洞攻防，在企业网站日益增加的今天，网管员通过本章可以了解 IIS 服务器的攻防问题。

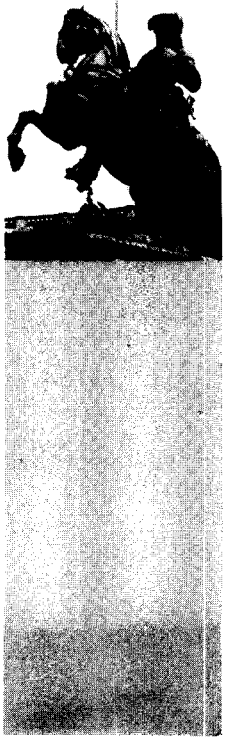
实战篇

- 瞒天过海：网游黑客：介绍常见的网络游戏盗号工具，以及一些网络游戏外挂作弊器，通过对具体的实例的学习，读者可以实现个人网游安全防护。
- 超级刺客：网络通讯：介绍常用聊天工具 QQ 和 MSN 的攻击原理和攻击方法，主要有 QQ 远程盗号木马的使用、“QQ 枪手”在线盗取密码、QQ 机器人盗号等具体实例。
- 黑虎掏心：电子邮箱：介绍电子邮箱密码的攻击与防范，主要包括破解 Web-Mail 邮箱密码、破解 POP3 邮箱密码，以及一些常见的电子邮箱欺骗攻击，如 TXT 文件欺骗、Outlook Express 漏洞欺骗等。
- 猛虎背袭：IE 浏览器恶意攻击：介绍针对 IE 浏览器的恶意攻击与防范，包括网页的恶意攻击、使用网页恶意代码修改系统信息，以及 IE 炸弹的攻击与防范。
- 杀出重围：网吧攻击：分析了到目前为止网吧攻击的有利条件，介绍了针对不同网吧代理服务器的攻击技巧，通过使用一些攻击工具，对网吧的万象服务器实施攻击。了解破解网吧服务器的技巧和原理，进而从中获得网吧安全防御的技巧。
- 乘虚而入：Windows 操作系统：介绍 Windows XP、Windows NT 及 Windows 2003 系统漏洞的攻防，通过实战完成各个漏洞的具体攻防。尽管各个系统的漏洞不同，攻击方式不同，但通过对本章的学习读者可以知其攻击原理，从而熟悉 Windows 操作系统漏洞攻防的具体方法。
- 移花接木:木马植入攻击：从木马的基本类型、伪装手段开始讲述，然后详细介绍了木马的植入和伪装方法的步骤，最后讲述了木马的清除和防范。
- 防不胜防：注入攻击：讲述注入攻击的基本原理和流程，并通过各种注入攻击的实战对注入攻击进行了深度剖析。
- 神兵利器：扫描、嗅探和欺骗：详细介绍了在黑客中经常使用的扫描和反扫描工具以及经典的嗅探器，并通过实例讲述了各个工具的具体使用方法。读者可以通过各个工具的具体功能来找寻合适的扫描工具。
- 铜皮铁骨：打造自己：主要介绍网络的安全防御，包括间谍软件的防御、流氓软件的清除、关闭端口和隐藏 IP 等方面。通过对本章知识的学习，读者可以不用再担心网络安全问题，任意遨游网络。
- 冥神护体：杀毒软件：介绍了多种比较经典的杀毒软件，如江民杀毒软件 KV2007、金山毒霸 2007 杀毒套装及瑞星杀毒软件 2007 等。读者可以通过具体的操作使用，选择合适的杀毒软件。

为区别于市场上同类的黑客类书籍，本书在写作上摒弃了同类书惯常采用的一本正经教学的方式，代之以谆谆善诱、可操作性极强的写作手法，使枯燥乏味的黑客攻防技术变得容易上手，让读者的网络安全实战技术随着对本书的阅读而渐入佳境。本书内容简洁、语言通俗易懂、思路清晰明朗，主要通过实际的攻击案例入手，来为读者讲述黑客攻防鲜为人知的秘诀，首先介绍黑客攻击的原理、流程和常用的攻击工具，从而探讨预防黑客的具体措施，接着针对各种各样具体模式的攻击，分别佐以相当详细的描述和解释，每一部分的内容都力求有攻有防，最后为了让读者对计算机安全技术的掌握有一个质的飞跃，专门介绍了多种反病毒软件的使用。

本书充分考虑了初学者的实际需要，对那些迫切想要实现保护电脑隐私、防病毒、防黑客的初级读者，希望可以通过学习本书能够轻松地掌握保护电脑隐私、防病毒、防黑客的方法，另外也兼顾了中高级读者的需求，可谓雅俗共赏。

本书由陈芳编写，作者抱着对读者极其尊重的心态写完此书，在写作的过程中紧紧围绕着本书的主旨思想，力求精益求精，但是由于互联网各项技术的飞速发展，任何一本电脑书籍，尤其是黑客类书籍，都很难保证书中所讲述的内容和实际应用中的操作完全一致，再加上作者水平有限，书中难免会有疏漏之处，望广大的读者多提宝贵意见！



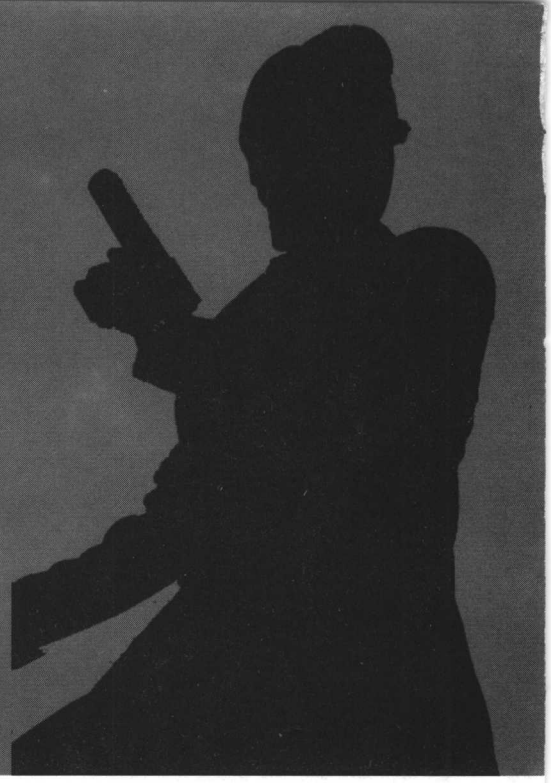
目　录

快速入门篇：黑骑士闭关修炼

实战篇：黑骑士驰骋沙场

第1篇

快速入门篇：黑骑士闭关修炼



第1章

黑客攻防基础修炼

学习目标

通过本章的教学，务求使读者掌握黑客攻击与防御的基础知识和技巧，掌握黑客攻击的具体流程和原理，熟悉扫描器、木马、破解软件以及炸弹等常见的攻击工具的功能和使用方法，从而认识到黑客预防的重要性，并从中找到预防黑客攻击的有效方法。

随着计算机技术的日益发展和完善，对计算机产品的安全要求也越来越迫切，强有力的计算机安全技术及安全产品如雨后春笋般出现，计算机的漏洞和缺陷越来越少。但与此同时黑客工具也在大肆传播，并且黑客工具发展的“简单化、自动化、傻瓜化”使得网络上的黑客攻击事件逐渐增多。

事物都是一分为二的，很多黑客工具在“红客”手中可以被用作扫描器，网络管理员可以用它来检查系统漏洞，防患于未然，而对于一些“黑客”来说，它是用来寻找攻击入口，为实施攻击做准备的。但是若单单只是利用工具去做一些攻击，知其然而不知其所以然，是不可能成为一个完全的“黑客”的。

1.1 攻击的流程和原理

从技术上说，黑客入侵的动机是成为目标主机的主人，只要能获得一台网络主机的超级用户权限，就可能在该主机上修改资源配置、安置“特洛伊”程序、隐藏行踪、执行任意进程等。

但要入侵总要有机可乘才行。虽然网络发展日益更新，然而网络中的安全漏洞却是不可避免的，即使旧的安全漏洞补上了，新的安全漏洞仍将不断出现，网络攻击正是利用这些存在的漏洞和安全缺陷对系统和资源进行攻击的。下面首先来介绍黑客攻击的基本流程，从零开始，了解攻击者是怎样一步步找到计算机中的安全漏洞并进行攻击的。

1. 黑客攻击的流程

隐藏自己的位置

一般攻击者都会利用别人的电脑来隐藏自己真实的 IP 地址，老练的攻击者还会利用 800 电话的无人转接服务连接 ISP，然后再盗用他人的账号。

寻找并分析目标主机

攻击者首先要寻找并分析目标主机，在 Internet 上 IP 地址是真正标识主机的，域名是为了方便记忆主机的 IP 地址而另起的名字，所以利用域名和 IP 地址就可以找到目标主机。当然，知道了要攻击目标的位置还远远不够，还必须对主机的操作系统类型及其所提供的服务等信息进行全面的了解。此时，攻击者可以使用一些扫描器工具，了解目标主机运行的是哪种版本的操作系统，系统有哪些账户，Web、FTP、Telnet、SMTP 等服务器程序版本等信息，为入侵做好充分的准备。

获取账号和密码，登录主机

攻击者在入侵一台主机前，首先要有该主机的一个账号和密码，否则连登录都无法进行，更不要说入侵了。如此就迫使攻击者先设法盗窃账户文件进行破解，从中获取某用户的账户和口令，再找寻合适时机以此身份进入主机。此外利用一些工具或系

统漏洞登录主机也是攻击者常用的一种方法。

获得控制权

攻击者使用 FTP、Telnet 等工具通过系统漏洞进入目标主机系统，获得控制权之后，首先要做两件事：清除记录和留下后门。此时需要更改某些系统设置，在系统中置入特洛伊木马或其他一些远程操纵程序，以便日后可以不被觉察的再次侵入系统。大多数后门程序是预先编译好的，只需要修改时间和权限就可以使用了，甚至新文件的大小都和原文件一模一样。攻击者一般使用 rep 传递文件，以免留下 FTP 记录。最后使用清除日志、删除拷贝的文件等方法来隐藏自己的踪迹，以便开始下一步的行动。

窃取网络资源和特权

攻击者找到攻击目标后，可以进行下一步的攻击，这也是攻击的目的所在。如：下载有用信息；实施窃取账号密码、信用卡号等经济偷窃；使网络瘫痪等。

2. 黑客攻击的原理和方法

熟悉攻击流程之后，下面就来了解常见的网络攻击原理和方法。

➲ 口令入侵

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。此种方法的前提是必须得到该主机上的某个合法用户的账号，然后再进行口令的破译。获得普通用户账号的方法很多：

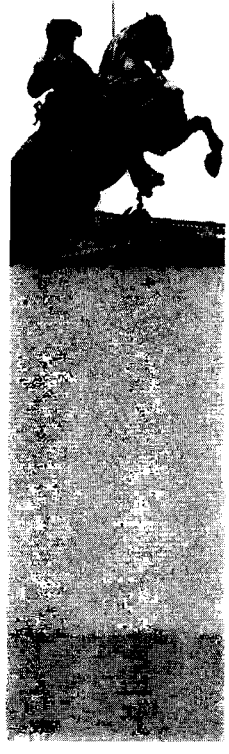
（1）从电子邮件地址中查询：有些用户的电子邮件地址常会透露其在目标主机上的账号。

（2）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，从而造成账号的泄露。

（3）通过网络监听非法得到用户口令：此种方法有一定的局限性，但危害性极大，监听者采用中途截击的方法获取用户账号和密码，当前很多协议根本就没有采用任何的加密或身份认证技术，如在 Telnet、FTP、HTTP、SMTP 等传输协议中，用户账号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即可轻松收集到账号和密码。

另一种中途截击攻击方法更为厉害，本机同服务器端建立连接之后，使用这种方法可以在通信过程中扮演“中间人”的角色，假冒服务器身份进行欺骗，再假冒本机向服务器发出恶意请求，其造成的后果无法估量。此外，攻击者还会利用软件或硬件工具不间断的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。

（4）知道用户的账号后利用一些专门软件强行破解用户口令：此种方法不受网段限制，但要求攻击者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，申请验证进入系统。若口令错误，就按序取下一个



单词进行尝试，并依次循环下去，直到找到正确的口令或字典中的单词试完为止。

(5)利用系统管理员的失误：在 UNIX 操作系统中，用户的基本信息存放在 passwd 文件中，所有的口令经过 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，会使用专门的破解 DES 加密法的程序来破解口令。此外，由于为数不少的操作系统都存在许多安全漏洞、Bug 或其他设计缺陷，这些缺陷一旦被找出，黑客就可以长驱直入。

➲ 安插特洛伊木马程序

特洛伊木马程序可以直接侵入用户的电脑并进行破坏，其时常被伪装成工具程序或者游戏程序，诱使用户打开，一旦用户打开或执行了这些程序，木马程序就会在计算机系统中隐藏一个可以在 Windows 启动时悄悄执行的程序。当用户连接到因特网上时，这个程序就会通知攻击者，报告用户的 IP 地址以及预先设定的端口。攻击者在收到这些信息后，利用这个潜伏着的程序，就可以任意地修改该计算机的文件设定、复制或删除文件以及更改硬盘内容等，从而达到控制计算机的目的。

➲ Web 欺骗技术

越来越多的用户利用 IE 等浏览器进行各种各样的对 Web 站点的访问，如查看新闻、查询商品、订阅报纸等。一般用户可能认为这些只是简单操作，不会有什么影响，而黑客正是通过篡改这些网页，而在用户打开篡改后的网页时得到相应的信息。

➲ 电子邮件攻击

电子邮件已成为一种基本的网络通讯方式，所以通过电子邮件攻击也成为一种常用的手段，相应的攻击方法一般有两种：

(1) 电子邮件炸弹：利用伪造的 IP 地址和电子邮件地址向同一信箱不间断的发送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，甚至使其瘫痪。

(2) 电子邮件欺骗：攻击者佯称自己为系统管理员，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）或在正常的附件中夹杂病毒或其他木马程序。

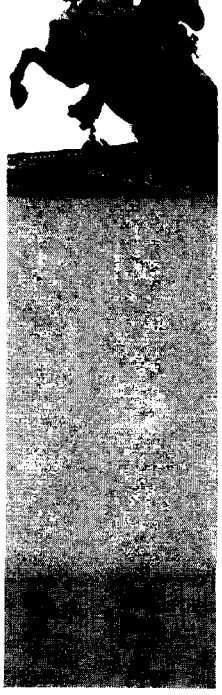
➲ 通过节点进行攻击

攻击者在成功攻击一台主机后，以此主机作为根据地，攻击其他主机，隐蔽其入侵路径，避免留下痕迹。同时可以使用网络监听方法，尝试攻破同一网络内的其他主机；或者通过 IP 欺骗与主机信任关系，攻击其他主机。

此类攻击十分隐蔽，攻击者通过外部计算机伪装成另一台合法机器来实现，其目的在于诱骗网络中的其他机器，将攻击者机器作为合法机器加以接受，从而进行数据发送或修改数据。其中 TCP/IP 诱骗可以发生 TCP/IP 系统的所有应用层上，包括数据链路层、网络层、传输层及应用层。如果底层受到侵害，则应用层的所有协议都处于危险之中。

➲ 网络监听

网络监听在网络中的任何一个位置下都可进行。在网络中，当信息进行传播的时候，利用工具将网络接口设置在监听的模式，便可将网络中正在传播的信息截获，从



而进行攻击，而黑客一般都利用网络监听来截取用户口令。

例如当有人攻占一台主机之后，若要再将战果扩大到这个主机所在的整个局域网中，监听往往是最佳选择，但运行已经被控制的主机上的监听程序，却是一件费神的事情，而且还需要攻击者有足够的耐心和应变能力。

➲ 后门软件攻击

后门软件攻击是互联网上比较多的一种攻击手法。BO2000、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，然后对其进行完全的控制，除了可以进行文件操作外，同时也可以进行桌面抓图、取得密码等操作。

这些后门软件分为服务器端和客户端，当黑客进行攻击时，会使用服务器端程序登录上已安装好客户端程序的电脑，这些客户端程序都比较小，一般附带于某些软件上，用户下载了一个小游戏并运行时，后门软件的客户端就很有可能神不知鬼不觉地安装成功了，而且大部分后门软件的重生能力比较强，给用户的清除造成了很大的麻烦。

➲ 拒绝服务攻击

实施拒绝服务攻击（DoS）的难度比较小，但破坏性却很大。具体手法就是向目的服务器发送大量的数据包，几乎占用了该服务器所有的网络带宽，从而使其无法对正常的服务请求进行处理，导致网站无法进入、响应速度大大降低或服务器瘫痪等后果。

现在常见的蠕虫类病毒都可以对服务器进行拒绝服务攻击。他们的繁殖能力极强，一般通过微软的 Outlook 软件向众多邮箱发出带有病毒的邮件，使邮件服务器无法承担如此庞大的数据处理量而瘫痪。

➲ 安全漏洞攻击

许多系统都有这样那样的安全漏洞（Bug），其中一些是操作系统或应用软件本身具有的，如缓冲区溢出漏洞。由于很多系统不检查程序与缓冲区之间变化的情况，就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做攻击的字符，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这一漏洞发动攻击，破坏根目录，从而获得超级用户的权限。

➲ 端口扫描攻击

端口扫描攻击是一种常用的探测技术，攻击者可将它用于寻找能够成功攻击的服务。连接在网络中的所有计算机都会运行许多使用 TCP 或 UDP 端口的服务，而所提供的已定义端口达 65535 个（即 256×256），端口扫描可让攻击者找到各种可用于发动攻击的端口。

端口扫描包括向每一个端口发送消息，每次只发一条，所接收到的响应类型表明该端口是否被使用，进而可以对其进行探测以寻找其弱点。对端口所进行的扫描通常发生在面向连接的 TCP 端口上，所以攻击者会得到有效的反馈信息。

1.2 常见的攻击工具

子曰：“工欲善其事，必先利其器”，只有合理的使用工具，才能有效、简捷的实现攻击的目的。下面就来具体了解各类攻击工具。

1. 扫描器

扫描器是自动检测远程或本地主机安全性弱点的程序。在 Internet 安全领域，扫描器是最出名的破解工具，而黑客手中的扫描器如同刺客手中之刀，可以“杀人”、“保命”、攻击、补漏。

真正的扫描器是 TCP 端口扫描器，这种程序可以选择 TCP/IP 端口和服务（例如 Telnet 或 FTP），并记录目标的应答。通过此种方法，可以搜集到关于目标主机的有用信息（例如匿名用户是否可以登录）。而其他所谓的扫描器仅仅是 UNIX 网络应用程序，这些程序一般用于观察某一服务是否正在一台远程机器上正常工作，并不是真正的扫描器，但也可以用于收集目标主机的信息（UNIX 平台上通用的 rusers 和 host 命令就是这类程序的很好的例子）。

➲ 扫描器应用平台

虽然扫描器程序一般是为 UNIX 工作站编写的，但现在已有了适用于任何操作系统的扫描器。

➲ 运行扫描器的系统要求

系统要求取决于扫描器、操作系统以及与 Internet 的连接方式。某些扫描器是专为 UNIX 编写的，所以需要 UNIX 系统。

➲ 扫描器运行目的

扫描器能够发现目标主机某些内在的弱点，这些弱点可能是破坏目标主机安全性的关键性因素。但是，要做到这一点，必须了解如何识别漏洞，许多扫描器没有提供多少指南手册和指令，因此熟悉数据的解释非常重要。

➲ 扫描器主要功能

扫描器主要有以下几种功能：

（1）寻找一台机器或一个网络；

（2）一旦发现一台机器，可以找出该机器正在运行的服务；

（3）测试具有漏洞的那些服务。

➲ 常用扫描器

黑客们实施攻击时，常用的扫描器主要有如下几种：

（1）Cerberus Internet Scanner（CIS）

该扫描器运行在 Windows NT 和 Windows 2000 平台下，所以主要针对微软的 Windows 操作系统进行探测扫描。CIS 拥有绝大多数菜鸟喜欢的友好的 Windows 界面，而且所提供的扫描安全问题也是在 Windows 中经常见到的。

其主要扫描以下项目：

- Web 服务；
- FTP 服务；
- SQL Server 数据库；
- NetBIOS 共享；
- 注册表设置；
- NT 服务漏洞；
- SMTP 服务；
- POP3 服务；
- RPC 服务；
- 端口映射；
- Finger 服务；
- DNS 安全；
- 浏览器安全。

在 CIS 各项功能中，最引人注目的是 NetBIOS 共享扫描。CIS 能根据 NetBIOS 这一漏洞作出 NetBIOS 资源信息、共享资源、计算机用户名、工作组和薄弱的用户口令等详细的扫描分析。

此工具容易操作，只需要输入目标服务器的地址，然后选择想要扫描的相关漏洞即可开始扫描，扫描完毕后会自动生成一个 HTML 的报告以便进行结果分析。

（2）X-Scanner

X-Scanner 运行在 Windows 平台下，主要针对 Windows NT/2000 操作系统的安全进行全面细致的评估，可以扫描出很多 Windows 系统流行的漏洞，并详细指出安全的脆弱环节与弥补措施。X-Scanner 采用多线程方式对指定的 IP 地址段或单机进行安全漏洞扫描，支持插件功能，提供了图形界面和命令行两种操作方式，是攻击者最为常用的工具之一。

主要扫描以下项目：

- 标准端口状态及端口 banner 信息；
- CGI 漏洞；
- RPC 漏洞；
- SQL Server 默认账户；
- FTP 弱口令；
- NT 主机共享信息；
- 用户信息；
- 组信息；
- NT 主机弱口令用户等。

扫描结束后，X-Scanner 会将扫描结果保存在 log 目录中，index_*.htm 为扫描结果索引文件。对于一些已知漏洞，X-Scanner 将给出相应的漏洞描述、使用程序及解

决方案。X-Scanner 扫描的内容是大部分服务器容易出现的漏洞和安全设置问题，其中常用的是 SQL 默认账户、FTP 弱口令和共享扫描，可以揭露网管所犯的一些低级错误。

下面来熟悉一下 X-Scanner 的具体使用流程：

X-Scanner 包括两个运行程序：xscan.exe 和 xscan_gui.exe，如图 1-1 所示。这两个程序分别是扫描器的控制台版本和窗口版本，初学者可能更容易接受窗口版本的扫描软件，因为毕竟初学者使用最多的是“窗口程序”，但无论运行那一个版本，它们的具体功能都是一样的。

运行窗口版本打开如图 1-2 所示的窗口。由图可以看到窗口分为左右两部分：左面是进行扫描的项目，包括前面提到的漏洞扫描、端口扫描等基本内容；另一部分是有关扫描范围的设定，X-Scanner 支持对多个 IP 地址的扫描，即使用者可以利用 X-Scanner 成批扫描多个 IP 地址，例如在 IP 地址范围内输入 202.0.0.1-202.0.0.255 就会扫描此网段的 255 台计算机，此时黑客可以针对某一个漏洞进行搜索，找到该范围内所有存在此漏洞的计算机。

图 1-1

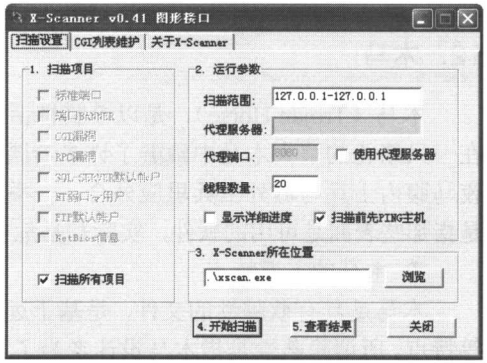


图 1-2

下面进行一个简单的标准端口扫描，扫描 IP 地址范围为 222.85.124.1-222.85.124.155，如图 1-3 所示。单击【开始扫描】按钮打开如图 1-4 所示的窗口，显示扫描进程。

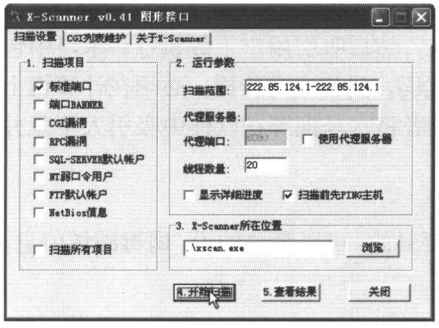


图 1-3

图 1-4