黑客攻防

实战必备

科教工作室 编著

剖析黑客常用攻击工具和攻击手段，消除各种漏洞隐患，增强安全保护措施，掌握防范黑客攻击的有效方法，消灭入侵的黑客。让您的电脑无懈可击！

使用各种加密工具加密电脑中的系统文件、Office文档、压缩包、应用程序以及驱动器，设置BIOS密码、系统启动密码、屏幕保护程序密码、电源管理密码，备份重要数据……实现对电脑的完全控制。让您的电脑牢不可破！

掌握防范间谍软件、木马程序和病毒的有效方法，安装高效的防毒杀毒程序，建立系统化的安全防御机制，做好上网时的安全防御和监控。让您的电脑百毒不侵！

清华大学出版社

黑客攻防实战必备

科教工作室　编著

清華大學出版社
北京

内 容 简 介

知己知彼，方能百战不殆。本书由浅入深、系统全面地介绍了计算机黑客攻防的实战知识，详细剖析了黑客攻防时的方法、工具及技巧，能帮助你全面解决网络安全的烦恼。

本书共分为14章，涵盖了黑客攻防入门、黑客常用攻击工具揭秘、安全检测工具解析、搜集与分析主机信息、服务器攻防、远程控制攻防、数据安全攻防、Windows 7系统安全攻防、聊天软件攻防、浏览器攻防、电子邮件攻防、木马攻防、计算机病毒攻防、手机攻防等内容。

本书内容丰富、方案详尽、实用性强，有助于所有上网用户提高网络安全意识，是专业网络安全人员不可缺少的参考书。

图书在版编目(CIP)数据

黑客攻防实战必备/科教工作室编著. --北京：清华大学出版社，2012
ISBN 978-7-302-29365-1

Ⅰ. ①黑…　Ⅱ. ①科…　Ⅲ. ①计算机网络—安全技术　Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2012)第158237号

责任编辑：章忆文　杨作梅
封面设计：杨玉兰
责任校对：王　晖
责任印制：张雪娇

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62791865

印 装 者：三河市李旗庄少明印装厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：24.5　　**字　　数**：515千字
版　　次：2012年8月第1版　　**印　　次**：2012年8月第1次印刷
印　　数：1～4000
定　　价：43.00元

产品编号：042598-01

前　言

随着网络技术的发展和进步，因特网已逐渐融入人们的日常生活中，大家在享受因特网所带来的便捷的同时，隐藏在它背后的阴影也开始慢慢地凸现出来。目前，越来越频繁的有预谋、有组织、有针对性的黑客多样化攻击和破坏活动不断发生，其攻击力不断增强，影响也越来越大。

但是，很多用户只具备计算机的使用技能，而对黑客攻击、防御等安全方面的知识不甚了解。实际上，作为一个计算机使用者，掌握一些抵御黑客攻防的技能是非常必要的。

为了让大家在较短的时间内就能快速提高计算机的安全防范意识和技能，我们编写了本书。本书共 14 章，由浅入深、循序渐进、系统全面地介绍了黑客攻防的理论知识、操作技巧及技术进阶和高级实战的演练，具有知识体系完整、技术内容新颖、实战案例丰富等特点，涵盖了黑客攻防入门、黑客常用攻击工具揭秘、安全检测工具解析、搜集与分析主机信息、服务器攻防、远程控制攻防、数据安全攻防、Windows 7 系统安全攻防、聊天软件攻防、浏览器攻防、电子邮件攻防、木马攻防、计算机病毒攻防、手机攻防等内容。从入门到精通，全面囊括！

本书语言简练、交互性强，采用直观图示的讲解方式，易教、易学、易用。适合以下读者阅读：

- 计算机初、中级用户。
- 喜爱研究黑客技术的网络用户。
- 专业网络安全维护技术人员。
- 专业系统维护技术人员。
- 大中专院校相关专业的师生。

本书由科教工作室组织编写，韩春、高尚兵、陈胜尧、崔浩、丁永平、费容容、黄纬、蒋鑫、李青山、刘兴、倪震、孙美玲、谭彩燕、王佳、王经谊、俞娟、张蓓蓓、张魁、周慧慧、朱俊等人也参与了创作和编排等事务。

由于作者水平有限，书中难免有不妥之处，欢迎广大读者批评指正。另外，如果你在使用本书时有任何疑难问题，可以通过邮箱(kejiaostudio@126.com)与我们联系，我们将尽全力解答你所提出的问题。

科教工作室

警告：本书仅以学习技术实务的角度来提醒读者如何加强自己的防黑观念与知识，从而将黑客拒之门外。根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，读者若将本书内容用于任何违反法律之行为，必须自行承担相应的法律责任，请各位读者慎之！

目　录

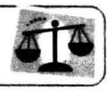
第1章　黑客攻防入门

随着网络的广泛应用，网络在方便人们日常生活、工作的同时，网络安全问题也得到越来越多人的关注。为此，本章将重点介绍黑客攻防必备知识、计算机漏洞、黑客攻击常用工具以及日常计算机防护的一些实用、有效的技巧，为后面学习黑客攻防技术奠定基础。

本章主要内容

- 揭开黑客的面纱
- 计算机系统漏洞分析
- 了解黑客的攻击行为
- 黑客攻防常见术语

1.1 揭开黑客的面纱



在过去的几年中，因特网的迅速发展使整个世界发生了前所未有的变化，人们在享受因特网所带来的便捷的同时，隐藏在它背后的阴影也开始慢慢地凸现出来。有这样一群人，他们潜伏在因特网中，窥探他人的隐私，窃取机密文件，破坏计算机系统。他们就是黑客。本书将为大家揭开黑客的神秘面纱。

1.1.1 剖析黑客

黑客 (Hacker)最早出现于 20 世纪 50 年代，在麻省理工学院 (MIT) 中有一批计算机迷自称 Computer Hacker，他们编制出第一个游戏程序《空间大战》，随后出现了象棋程序、在分时系统网络里给别人留言的软件等。MIT 的黑客属于第一代。

20 世纪 60 年代中期，起源于 MIT 的“黑客文化”开始弥漫到美国其他校园，并逐渐向商业渗透，黑客们开始进入或建立电脑公司。其中最著名的有贝尔实验室的邓尼斯·里奇和肯·汤姆森，他俩在小型电脑 PDP-11/20 上编写出 UNIX 操作系统和 C 语言，推动了工作站电脑和网络的成长。MIT 的理查德·斯德尔曼后来发起成立了自由软件基金会，成为国际自由软件运动的精神领袖，他们都是第二代黑客的代表人物。

自 20 世纪 70 年代起，黑客逐渐走向反面，开始在网络上利用技术危害他人。例如，约翰·达帕尔编制的“嘎吱船长”口哨玩具，吹出的哨音可以开启电话系统，进行免费的长途通话；世界头号黑客凯文·米特尼克曾侵入美国多家大公司，偷窃和修改数以千计的重要文件，非法使用 2 万多张信用卡。

20 世纪 80 年代初期，计算机地下组织开始形成，出现了早期的计算机窃贼。例如，德国汉堡一个名叫“混沌”的计算机俱乐部(CCC)的成员通过网络将 10 万美元自汉堡储蓄银行转到 CCC 账号上。

在 20 世纪 80 年代末期，出现了第一个蠕虫病毒——莫里斯蠕虫，它造成了 6000 多台计算机瘫痪，直接经济损失接近 1 亿美元，造成了美国高科技术史上空前规模的灾难事件。

21 世纪，黑客又发动了另一波计算机病毒蔓延的狂潮。例如，在 2000 年发动了一场黑客战争，把整个网络搅了个天翻地覆。同年 5 月，一种名为“爱虫”的病毒使数以千计的计算机系统瘫痪，造成的损失高达 100 亿美元。这引燃了全世界反黑客、反病毒的斗争激情。

2006 年年底，我国互联网上大规模爆发“熊猫烧香”病毒及其变种，该病毒通过多种方式进行传播，并将感染的所有程序文件改成熊猫举着三根香的模样，使受感染计算机出现蓝屏、频繁重启等状况。同时该病毒还具有盗取用户游戏账号、QQ 账号等功能。据统计，该病毒使北京、上海、广东等多个省市的计算机用户遭受感染，数百万台计算机被破坏。

如今的黑客已是为了牟取暴利而散发木马的“毒客”占主流，出现以赢利为目的、专业及组织化的恶意软件“产业”，他们在黑市公开销售。

1.1.2 黑客入侵的缘由

如今的黑客，攻击他人计算机的理由可谓是五花八门，可概括为以下几种原因：

(1) 想在别人面前炫耀自己的技术，比如进入心仪的女孩子的机器上修改一个文件或目录名，算是打个招呼，给朋友一个惊喜。

(2) 好玩、恶作剧、练功是许多人或学生入侵或破坏网络的最主要原因。除了有练功的效果外，还有些许网络探险的感觉。例如看不惯同事(同学)的某些做法，又不便当面指责，于是攻击他的计算机，更改他的桌面，更有甚者获得他的隐私，在适当的时机揭他的老底，让他难堪。

(3) 窃取数据，偷取硬盘中的文件或各种上网密码，然后从事各种商业应用，恶念偷窃银行存款等。抗议与示威，这是敌对国及敌对势力之间常出现的黑客行为。例如 2001 年 5 月 1 日中美黑客大战，两国的黑客互相攻击对方网站，轻者被篡改主页面，严重的则整个系统遭受毁灭性打击。

当然，不排除某些人仅仅只是出于好奇而并不是想达到任何目的。

1.1.3　了解黑客攻击流程

黑客攻击的流程如下。

1. 确定攻击目标

在进行攻击前，黑客会锁定要攻击的范围，比如要攻击哪个网段或哪台服务器，这样才会有针对性地渗透，也可以节省分析的时间。

2. 网络映射及踩点

黑客会获取待入侵网段或服务器的操作系统版本，开放服务的 banner 等。

3. 漏洞扫描

黑客会启动本机的扫描工具，对该网段的服务器进行漏洞扫描，找出安全隐患所在。

4. 获取目标系统的访问权

黑客通过扫描工具的最终扫描报告，分析出可利用的安全隐患，并利用该安全隐患，取得目标系统的普通权限。

5. 提升权限，获取控制权

黑客此时已经取得目标服务器的普通权限，但黑客最终的渗透目的是取得系统级权限，所以黑客通过本地提升程序，把权限提升到系统级权限，以便完全控制服务器。

6. 消灭踪迹

黑客在此前的漏洞攻击过程中，在目标服务器的日志里留下了很多痕迹。黑客此时要把这些痕迹清除掉，不被管理员发现。

7. 安装后门

黑客为了能够长时间地控制目标服务器，会在目标服务器里安装一款隐蔽且强大的后门，以方便下次进入。

8. 转移目标

黑客以后会以这台服务器为跳板，从这台服务器发起对其他服务器的攻击。

1.2 计算机系统漏洞分析

利用已知的程序漏洞进行攻击是黑客常用的方法。本章将对漏洞的性质和分类进行简要的介绍，并对一些常见的漏洞进行讲解，使读者对黑客攻防的基础知识有一个初步的了解。

1.2.1 计算机漏洞的性质

计算机系统其实并不如大家所想象的那么安全，随着互联网的飞速发展，计算机系统中的漏洞已越来越引起人们的重视，而针对这些漏洞的攻防技术始终在不断的变化中。

网络信息系统由硬件和软件组成，由于软件程序的复杂性和编程的多样性，在网络信息系统的软件中很容易有意或无意地留下一些不易被发现的安全漏洞，这些漏洞显然会影响网络信息的安全保密性，黑客往往通过这些安全漏洞来入侵和破坏网络信息系统。

漏洞是指任意地允许非法用户未经授权获得访问或提高其访问权限的硬件或软件特征。每个网络系统平台无论是硬件还是软件都存在漏洞，而且每个漏洞(或大或小)在整个网络系统中都是一个环节，破坏一个环节，攻击者就有希望破坏所有其他的环节，因此网络系统的漏洞具有连锁效应。

在目前经常使用的网络系统中，存在着大量的漏洞。在 2000 年，大约有 800 多个各种操作系统和应用软件的安全漏洞不断被公开和揭露，比 1999 年增加了 10%左右，并且这个数目呈加速增长的趋势。到 2001 年，平均每天有 4 个漏洞被公布。

1.2.2 计算机漏洞分类

1. 按照漏洞成因以及严重程度分类

对系统造成直接威胁的分类如下：

(1) 远程管理员权限。
(2) 本地管理员权限。
(3) 普通用户访问权限。
(4) 权限提升。
(5) 读取受限文件。
(6) 远程拒绝服务。
(7) 本地拒绝服务。
(8) 远程非授权文件存取。
(9) 口令恢复。
(10) 欺骗。
(11) 服务器信息泄露。

2. 按漏洞的成因来分类

(1) 输入验证错误。
(2) 访问验证错误。
(3) 竞争条件。

(4) 意外情况处置错误。

(5) 设计错误。

(6) 配置错误。

(7) 环境错误。

3. 按漏洞的严重程度来分类

A 类漏洞：威胁性最大的漏洞，往往由较差的系统管理或错误设置造成。

B 类漏洞：较为严重的漏洞，例如允许本地用户获得增加的和未授权的访问。

C 类漏洞：严重性不是很大的漏洞，例如允许拒绝服务的漏洞。

1.3 了解黑客的攻击行为

网络的开放性决定了它的复杂性和多样性，使得黑客攻击行为也变得复杂、多样化。那么，黑客都有哪些常用的攻击行为呢？这就是本章要介绍的内容。

1.3.1 黑客查找目标的方式

黑客选择下手目标时，会把攻击目标分为特定目标和任意目标两种。

1. 特定目标

特定目标是指已有攻击对象，这些攻击对象可能是仇家，也可能是对某人看不顺眼，或者纯属恶作剧、好玩等。通常可经由下列方式来找出下手目标的 IP 地址或者直接使用电子邮件地址进行入侵或攻击。

(1) 若入侵对象是一般上网用户，而且有固定的 IP 地址，则可以进行入侵、攻击或其他行为。

(2) 若入侵对象是一般上网用户，但并没有固定的 IP 地址，则必须查出对方当前上网的 IP 地址后才可以进行入侵或攻击，或者使用电子邮件地址来进行入侵或攻击。

(3) 若入侵对象使用 QQ，则可以通过 QQ 来找到对方当前的上网 IP 地址，然后再进行入侵或攻击。

(4) 若入侵对象是在因特网上的某个服务器或某个网页，则多半可以通过网址或域名查出它的 IP 地址，详细的操作说明见后面。

(5) 若无法找到对方真正的 IP 地址或对方当前根本没有上网，则可以通过电子邮件地址进行入侵与攻击，可参见后面开始入侵与攻击中所介绍的有关电子邮件入侵或攻击的各种方法。

2. 任意查找目标

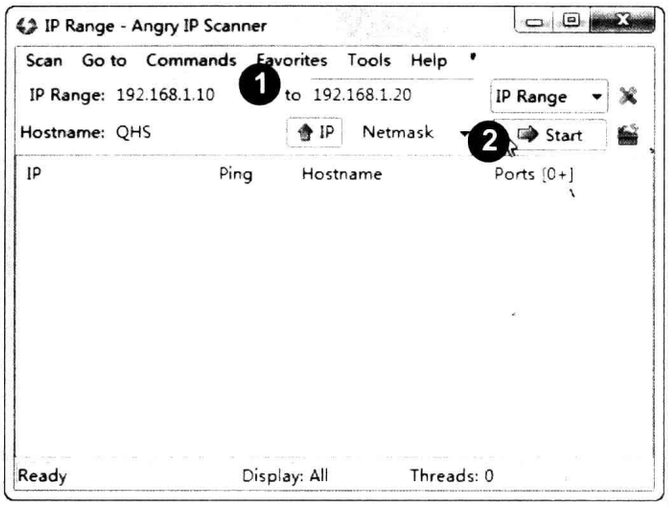
有些黑客只是闲来无事才去攻击别人，这时就会随意选择下手的目标了。最常用的方法是使用 IP 扫描工具来找出下手目标的 IP 地址，或者随手抓个电子邮件地址，然后使用工具进行入侵与攻击。

下面以 IP 扫描软件 Angry IP Scanner 为例做说明。它是一个相当小的 IP 扫描软件，但是其功能非常强大，可以在最短的时间内扫描远端主机 IP 的运作状况，并且快速地将结果

整理完回报给用户知晓。具体使用方法如下。

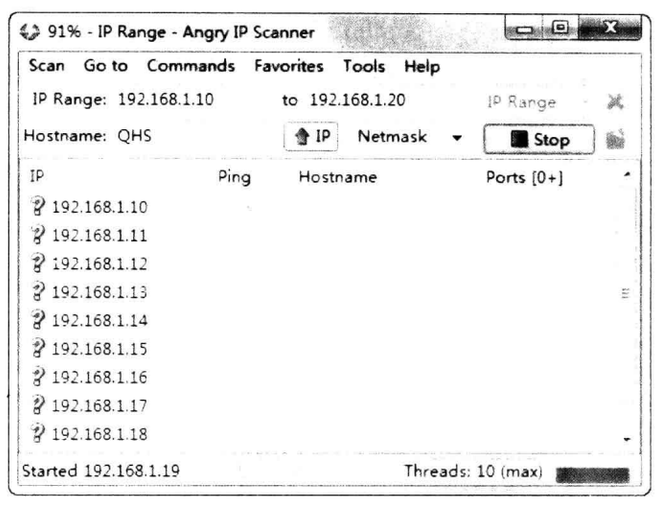
步骤 01 设置要扫描的 IP 地址段。

安装并启动 Angry IP Scanner 程序，然后在 IP Range 文本框中输入 IP 地址段，如下图所示。



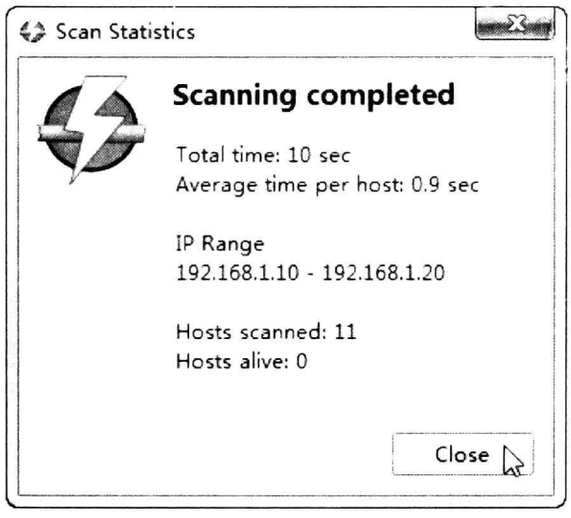
步骤 02 解析所输入的 IP 地址段。

单击 Start 按钮，即可开始扫描解析所输入的 IP 地址段，如下图所示。



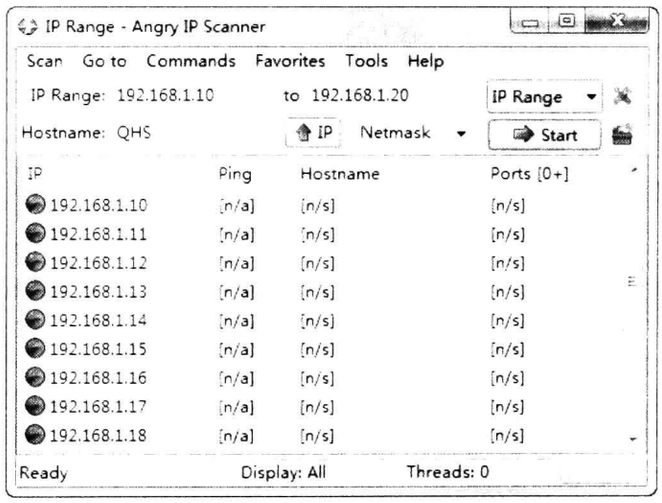
步骤 03 关闭 Scan Statistics 对话框。

扫描结束后弹出 Scan Statistics 对话框，提示扫描结果，单击 Close 按钮，如下图所示。



步骤 04 查看解析结果。

返回 Angry IP Scanner 窗口，即可在列表中查看分析结果，如下图所示。



1.3.2 进行系统踩点

对一个机构的系统进行踩点，可使攻击者了解该机构的安全态势。通过使用工具，攻击者能够由一个未知量(例如某家公司的因特网连接)归纳出域名、网络块以及直接连到因特网上的系统的个别 IP 地址的一个特定范围。

尽管有许多类型的踩点方法，但它们基本上以达到发现与这些技术相关的信息为目的：因特网、局域网、远程访问和外联网。下面集中讨论对一个机构的因特网连接的踩点。

步骤 01 确定活动范围。

步骤 02 网络踩点。网络踩点过程是标识与某个特定机构相关的域名和网络，域名代表公