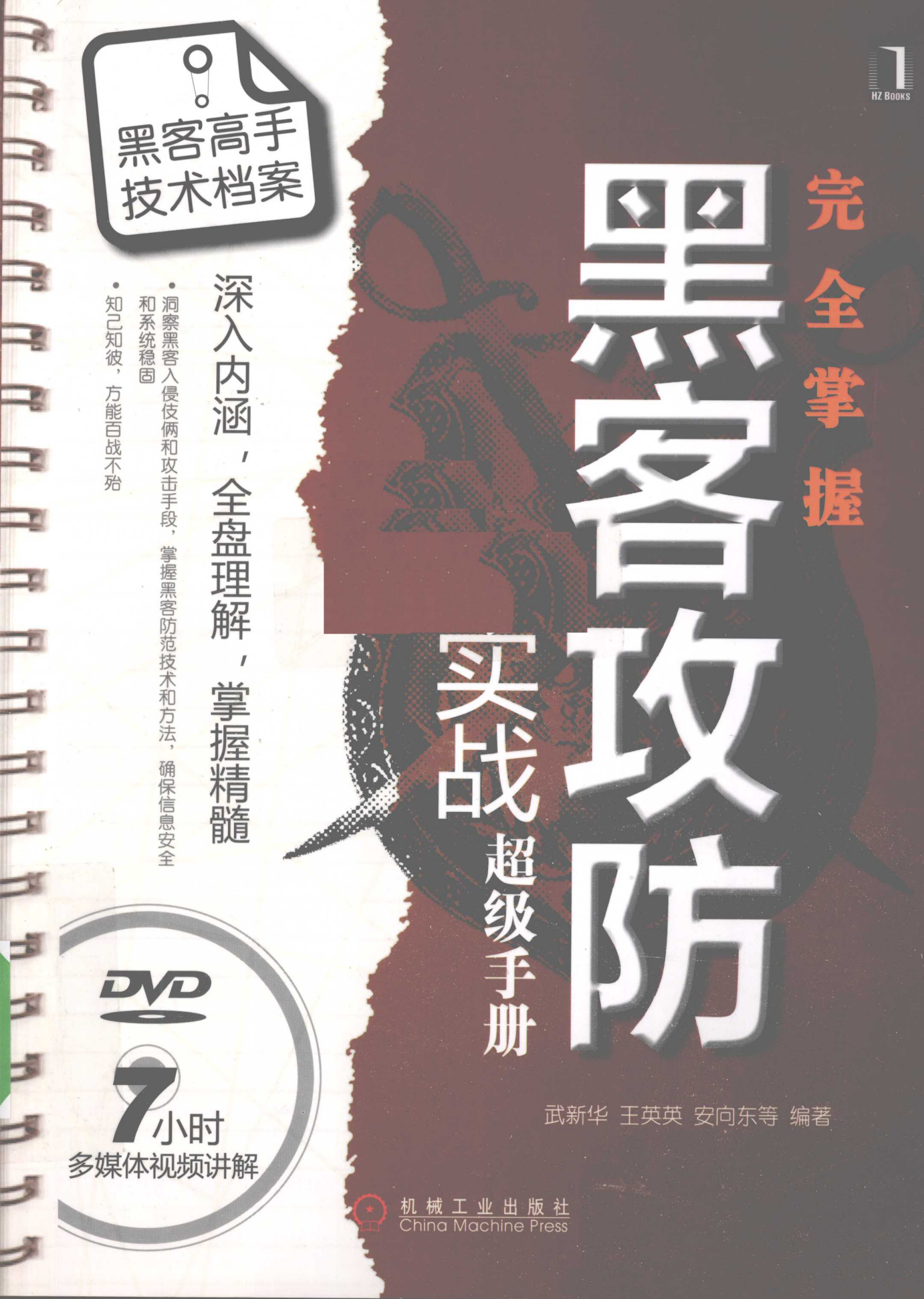
HZ BOOKS
黑客高手
技术档案
完全掌握
黑客攻防
实战超级手册
深入内涵，全盘理解，掌握精髓
• 洞察黑客入侵伎俩和攻击手段，掌握黑客防范技术和方法，确保信息安全和系统稳固
• 知己知彼，方能百战不殆
DVD
7小时
多媒体视频讲解
武新华 王英英 安向东等 编著
机械工业出版社
China Machine Press

完全掌握
黑客攻防
实战超级手册

武新华 王英英 安向东 等编著

机械工业出版社
China Machine Press

本书从了解黑客攻击手段，达到完全掌握防范黑客攻击为目的。全书以“攻”、“防”两个不同的角度，介绍黑客攻击手段的同时，讲述相应的防范技术；通过模拟案例，图文并茂地再现了黑客入侵网络与防御的全过程。书中主要内容包括：黑客入侵准备、基于系统漏洞的入侵与防范、局域网攻防实例、QQ 攻防实例、邮件欺骗与轰炸、密码攻防实例、网游与网吧攻防实例、手机病毒防范与清除、网银炒股安全实战、网站、数据库与服务器攻防、揭秘留后门与清脚印伎俩、揭秘自行制造病毒、解密黑客入侵与检测、备份升级与数据恢复、网络安全与防范。

本书突出任务驱动与案例教学，并配合长达 7 小时的多媒体视频教学，适合具有一定安全基础知识和工具使用基础的读者、网络管理人员、黑客技术爱好者阅读和参考。

图书在版编目（CIP）数据

完全掌握黑客攻防实战超级手册/武新华，王英英，安向东等编著.—北京：机械工业出版社，2010.5

ISBN 978-7-111-30361-9

I．①完… II．①武… ②王… ③安… III．①计算机网络－安全技术－手册 IV．①TP393.08-62

中国版本图书馆CIP数据核字（2010）第064418号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）
责任编辑：夏非彼　　迟振春
北京科普瑞印刷有限责任公司印刷
2010年5月第1版第1次印刷
188mm×260mm • 30.5印张
标准书号：ISBN 978-7-111-30361-9
　　ISBN 978-7-89451-490-5（光盘）
定价：58.00元（附1DVD）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991；82728184
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）82728184；88379603
读者信箱：booksaga@126.com

前言

本书从了解黑客攻击手段，达到掌握防范黑客攻击为目的。全书围绕“攻”、“防”两个不同的角度，介绍黑客攻击手段的同时，讲解了相应的防范方法；通过模拟案例，图文并茂地再现了黑客入侵网络与防御的全过程。

本书内容

- 介绍黑客攻击入侵手段与具体防范的方法和技巧，通过典型生动的案例向读者展示了多种黑客破坏性的攻击方法和工具的使用；
- 以深入剖析黑客入侵过程为主线来展开全书内容，向读者讲述入侵者是如何实现信息的搜集；
- 告知黑客是如何通过获取的信息打开目标服务器的切入点（基于身份验证、漏洞、木马等入侵手段）；
- 介绍黑客是如何实现入侵，即远程连接，入侵后如何执行各种任务；
- 讲解黑客是如何留下后门达到再次进入系统的目的；入侵者如何清除系统日志防止目标服务器发现入侵的痕迹。

本书最主要的精髓在于知己知彼，方能百战不殆。希望读者能够运用书中所揭示的黑客攻击防守方法去了解黑客，进而达到防范黑客攻击的目的，使自己的网络系统更加安全、稳固。

注　意：书中所有实例写作是在一个模拟的局域网内调试通过的。

本书特色

本书以场景式教学、案例驱动与任务进阶为写作特色，在书中可以看到一个个生动的场景案例。通过完成一个个任务的实践，读者不仅可以轻松掌握有关网络安全的知识，还可在不知不觉中快速提升网络安全防范的实战技巧。

- 场景式教学：紧扣“理论+实战，图文+视频=全面提升学习效率”的主导思想，采用最为通俗易懂的图文解说，为读者展示操作流程。
- 案例驱动：盘点最新黑客技术，并采用你攻我守的方法详述范例完整操作过程，便于读者实战演练。
- 任务进阶：详细分析每一个黑客入侵步骤，推断入侵者的每一入侵步骤的目的及所要完成的任务，并对入侵中的主要问题作必要的说明与解答。

每个专题都涉及黑客的攻击手段、造成的严重后果，以及如何预防，使其转危为安，最终挽回损失。每个专题给出具体案例，都是耳熟能详且

与现实生活息息相关的典型代表。

读者对象

本书涉及面较广，可作为一本黑客攻防技术的速查手册，也适合如下读者学习使用：

- 网络管理人员；
- 喜欢研究黑客技术者；
- 系统维护人员和电脑爱好者；
- 大中专院校相关专业的学生。

增值服务

随书附赠的 DVD 光盘提供了多种攻防实战的教学视频，汇集了众多高手的操作精华，通过增加读者对主流操作手法感性的认识，使读者提高防范技能，确保自己的系统安全。

此外，如发现本书中有不妥或需要改进之处，还可通过访问 http://www.newtop01.com 与笔者进行沟通，并真心希望在和广大读者互动的过程中能得到提高。

本书编者

本书作者长期从事网络安全管理工作，具有较强的实践操作能力及一线拼杀经验，可带领广大技术者穿越迷雾，把黑客们的伎俩侦察得清清楚楚。在本书的编写中：冯世雄负责第 1 章，张晓新负责第 2 章，陈艳艳负责第 3 章，李防负责第 4 章，余建国负责第 5、6 章，王肖苗负责第 7 章，孙世宁负责第 8 章，杨平负责第 9 章，段玲华负责第 10 章，李伟负责第 11 章，王英英负责第 12 章，郑静负责第 13 章，刘双红负责第 14 章，安向东负责第 15 章，最后由武新华通审全稿。我们虽满腔热情，但限于自己的水平，书中仍难免有失误、遗漏之处，我们心存谨敬，随时恭候您提出宝贵意见。

最后，需要提醒读者的是：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，否则后果自负。

编者

2010.04

目录

第1章

黑客入侵准备

重点提示

- 探测操作系统
- 探测网站信息及搜索引擎
- 扫描和嗅探实例分析

本章精粹

本章主要介绍黑客入侵前的准备工作，黑客入侵成功与否都不是偶然的，在入侵前的准备工作将直接影响着入侵的结果。入侵前的准备工作包括：探测系统、网站信息探测、搜索引擎探测、信息的筛选、网络监听与嗅探等，所以读者了解此内容后，可提早对黑客进行防范。

通常情况下，黑客在进行攻击之前都需要对目标进行全方位分析，当分析出的数据达到攻击条件之后，黑客便会主动攻击，并会在最短时间内攻破目标。因此，黑客攻击前的信息搜集的工作是最重要的，往往需要几个小时甚至几十个小时，越成熟的黑客在信息搜索上花费的时间就越多，攻击成功的几率也就越大。

1.1 探测操作系统

当黑客确定一个攻击目标时，首先会收集该目标电脑的信息，其中包括：安装的操作系统、启用的服务、开放的端口、管理员登录口，甚至有时还需要调查系统或网络管理员的私人信息，如电话、生日、姓名等。在收集信息时先要确定对方的操作系统，因为对于不同类型、不同版本的操作系统，系统漏洞区别很大，直接关系到黑客攻击时所使用的方法。此外，同一类型及版本的操作系统，由于安装的补丁包版本的不同，也决定着黑客攻击的失败与否。下面介绍几种适合防范者掌握的黑客使用的探测方法，帮助大家及早防范黑客入侵。

1.1.1 使用 X-Scan 探测

X-Scan 是一款扫描软件，可采用多线程方式对指定单机或 IP 地址段进行漏洞扫描，也支持插件功能。它基于图形界面与命令行两种操作方式，直观明了、简单易学。

下面以 X-Scan v3.3 为例介绍其具体的操作步骤：

Step 01 双击“X-Scan”应用程序，即可打开【X-Scan v3.3】主窗口，在【普通信息】选项卡中显示了该软件的使用说明，如图 1-1 所示。

Step 02 选择【设置】→【扫描参数】菜单项，即可打开【扫描参数】对话框，在其中选择【检测范围】选项，在右侧设置面板中指定要扫描目标计算机的 IP 地址，如图 1-2 所示。

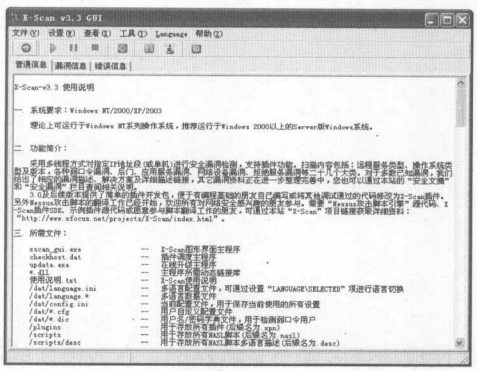

图 1-1 【X-Scan v3.3】主窗口

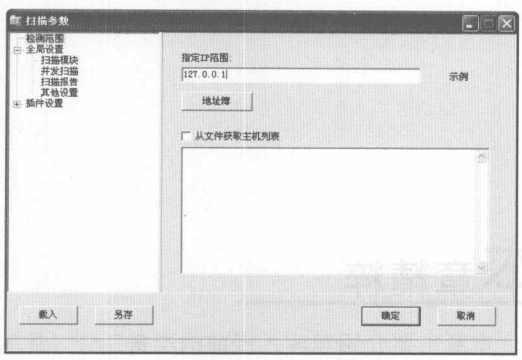

图 1-2 设置【检测范围】

Step 03 依次展开【全局设置】→【扫描模块】选项，在中间的设置面板中勾选“远程操作系统”复选框，如图 1-3 所示。

Step 04 选择【扫描报告】选项，即可在右侧设置面板中选择报告结果的方式。报告文件的生成方式有两种：HTML 文件和 TXT 文件，可根据情况进行选择，如图 1-4 所示。