ATTACK

在攻与防的对立统一中
寻求技术突破

黑客攻防
从入门到精通

Web脚本编程篇·全新升级版

明月工作室 马琳◎编著

超值赠送

黑客攻防全能视频+计算机硬件管理超级手册+Windows文件管理高级手册+Linux命令应用大全

以下人群请勿翻阅本书：

1.自以为很牛，对黑客不屑一顾的人
2.心存侥幸，认为黑客离自己很远的人
3.习惯黑客攻击，总是折腾他人的人
4.号太多，习惯被盗号的人
5.不差钱，不怕被盗刷的人
6.我不是Boss，对交易安全漠不关心的人

DEFENSE

北京大学出版社
PEKING UNIVERSITY PRESS

黑客攻防
从入门到精通
Web脚本编程篇·全新升级版

明月工作室 马琳◎编著

北京大学出版社
PEKING UNIVERSITY PRESS

内 容 提 要

本书由浅入深、图文并茂地再现了 Web 脚本编程方面的相关知识。

全书共 12 章，分别为黑客攻防入门、黑客的攻击方式、后门程序编程基础、高级系统后门编程技术、脚本编程攻防初级入门、黑客程序的配置和数据包嗅探、编程攻击与防御实例、SQL 注入攻击、网站数据库入侵、Cookies 攻击、恶意网页代码攻防、网络与 Wi-Fi 的攻防。

本书适用于计算机初中级用户、计算机维护人员、IT 从业人员以及对黑客攻防与网络安全维护感兴趣的计算机用户，也可以作为计算机培训班辅导用书。

图书在版编目(CIP)数据

黑客攻防从入门到精通. Web脚本编程篇 : 全新升级版 / 明月工作室, 马琳编著. — 北京 : 北京大学出版社, 2017.2

ISBN 978-7-301-27849-9

Ⅰ. ①黑… Ⅱ. ①明… ②马… Ⅲ. ①黑客—网络防御 Ⅳ. ①TP393.081

中国版本图书馆CIP数据核字(2016)第296822号

书　　名： 黑客攻防从入门到精通（Web脚本编程篇 · 全新升级版）

HEIKE GONGFANG CONG RUMEN DAO JINGTONG

著作责任者： 明月工作室　马琳　编著

责 任 编 辑： 尹　毅

标 准 书 号： ISBN 978-7-301-27849-9

出 版 发 行： 北京大学出版社

地　　址： 北京市海淀区成府路205 号　100871

网　　址： http://www. pup. cn　　新浪微博: @ 北京大学出版社

电 子 信 箱： pup7@ pup. cn

电　　话： 邮购部62752015　发行部62750672　编辑部62580653

印 刷 者： 三河市博文印刷有限公司

经 销 者： 新华书店

787毫米 × 1092毫米　16开本　27印张　587千字

2017年2月第1版　2017年2月第1次印刷

印　　数： 1-3000册

定　　价： 59.00 元

从 2003 年起，中国互联网逐渐找到了适合国情的商业模式和发展道路，互联网应用呈现多元化局面，电子商务、网络游戏、视频网站、社交娱乐等百花齐放。计算机技术及通信技术的进一步发展，持续推动着中国互联网新一轮的高速增长。到 2008 年，中国的网民数量已经达到 2.53 亿人，首次超过美国，跃居世界首位。

从 2009 年开始，移动互联网兴起；互联网与移动互联网共同营造了当前双网互联的盛世。网络已经成为个人生活与工作中获取信息的重要手段，网络购物也已经成为民众重要的消费渠道。当前，“互联网 +”的战略布局与工业 4.0 的深度发展，使国家经济发展、民众工作生活，都与网络安全休戚相关，一个安全的网络环境是必不可少的。

当前最大的问题是广大用户对网络相关软硬件技术的掌握程度远远不够，这就为不法分子提供了大量的机会，借助于计算机网络滋生的各种网络病毒、木马、流氓软件、间谍软件，给广大网络用户的个人信息及财产带来了巨大的威胁。

为提升广大民众对于计算机网络安全知识的掌握程度，做好个人信息、财产安全的防护，我们编写了这套“黑客攻防从入门到精通”丛书，本书为其中的《黑客攻防从入门到精通（Web 脚本编程篇 • 全新升级版）》分册。

丛书书目

黑客攻防从入门到精通（全新升级版）
黑客攻防从入门到精通（Web 技术实战篇）
黑客攻防从入门到精通（Web 脚本编程篇 • 全新升级版）
黑客攻防从入门到精通（黑客与反黑工具篇 • 全新升级版）
黑客攻防从入门到精通（加密与解密篇）
黑客攻防从入门到精通（手机安全篇 • 全新升级版）
黑客攻防从入门到精通（应用大全篇 • 全新升级版）
黑客攻防从入门到精通（命令实战篇 • 全新升级版）
黑客攻防从入门到精通（社会工程学篇）

本书特点

- 内容全面：涵盖了从计算机黑客攻防入门，到专业级的Web技术安全知识，适合各个层面、不同基础的读者阅读。
- 与时俱进：本书主要适用于 Windows 7 及更新版本的操作系统用户阅读。尽管本书中的许多工具、案例等可以在 Windows XP 等系统下运行或使用，但为了能够顺利学习本书全部的内容，强烈建议广大读者安装 Windows 7 及更高版本的操作系统。
- 任务驱动：本书理论和实例相结合，在介绍完相关知识点以后，即以案例的形式对该知识点进行介绍，加深读者对该知识点的理解和认知能力，力争彻底掌握该知识点。
- 适合阅读：本书摒弃了大量枯燥文字叙述的编写方式，而是采用了图文并茂的方式进行编排，以大量的插图进行讲解，可以让读者的学习过程更加轻松。
- 深入浅出：本书内容从零起步，步步深入，通俗易懂，由浅入深，使初学者和具有一定基础的用户都能逐步提高。

读者对象

- 计算机初、中级用户。
- 网店店主、网店管理及开发人员。
- 计算机爱好者、提高者。
- 各行各业需要网络防护的人员、中小企业的网络管理员。
- Web 前、后端的开发及管理人员。
- 无线网络相关行业的从业人员。
- 计算机及网络相关的培训机构。
- 大中专院校相关学生。

本书结构及内容

本书一共有 12 章，内容由浅入深，循序渐进，前后衔接紧密，逻辑性较强。

第 1 章　黑客攻防入门

第 2 章　黑客的攻击方式

第 3 章　后门程序编程基础

第 4 章　高级系统后门编程技术

第 5 章　脚本编程攻防初级入门

第 6 章　黑客程序的配置和数据包嗅探
第 7 章　编程攻击与防御实例
第 8 章　SQL 注入攻击
第 9 章　网站数据库入侵
第 10 章　Cookies 攻击
第 11 章　恶意网页代码攻防
第 12 章　网络与 Wi-Fi 的攻防

超值赠送资源

1. 黑客攻防全能视频

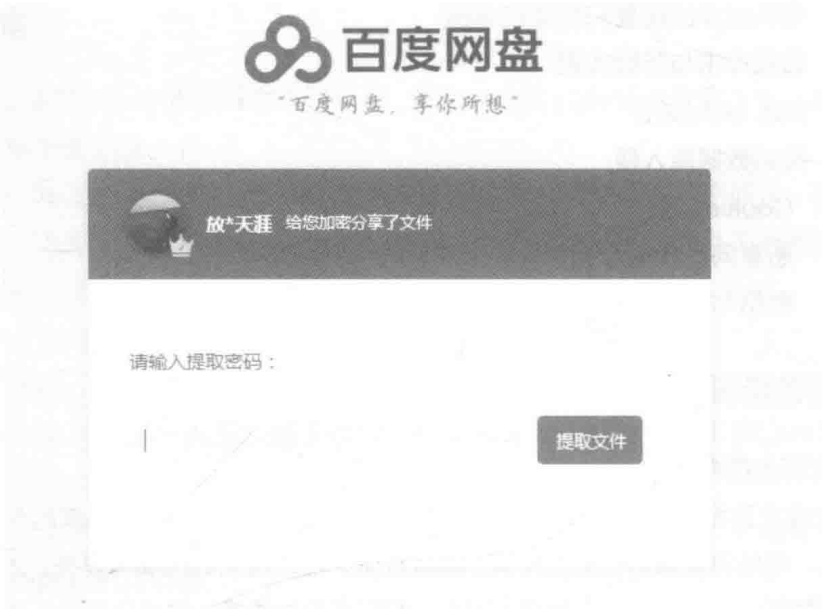
为了读者能全面地了解黑客方面的知识从而有效地防御黑客的不法入侵行为，本书特赠送全能教学视频，视频内容包括社会工程学、黑客攻防入门、信息的扫描与嗅探、木马与病毒的防范、系统漏洞防范、远程控制术、加密与解密、数据备份与恢复、移动网络安全等内容。

2. 其他赠送资源

- Windows 系统安全与维护手册
- 计算机硬件管理超级手册
- Windows 文件管理高级手册
- （140 个）Windows 系统常用快捷键大全
- （157 个）Linux 基础命令手册
- （136 个）Linux 系统管理与维护命令手册
- （58 个）Linux 网络与服务器命令手册
- 黑客攻防命令手册

我们已将赠送内容上传百度网盘，在浏览器中输入下载链接，打开链接后，在如下图所示的文本框中输入提取码便可下载赠送资源。下载链接：http://pan.baidu.com/s/1eSfvxDK，提取码：ez6a。

读者也可加入 QQ 群，在群文件中下载“资源下载地址列表”文档，直接复制链接和密码，下载多媒体视频。（注意：我们会在群文件中共享一些赠送资源，如百度网盘链接失效，请加入 QQ 群下载资源。）



后续服务

本书由马琳编著，胡华、王栋、宗立波、栾铭斌、赵玉萍、闫珊珊等老师也参加了本书部分内容的编写和统稿工作，在此一并表示感谢！在本书的编写过程中，我们竭尽所能地为您呈现最好、最全的实用功能，但仍难免有疏漏和不妥之处，敬请广大读者不吝指正。若您在学习过程中产生疑问或有任何建议，可以通过 E-mail 或 QQ 群与我们联系。

投稿信箱：pup7@pup.cn

读者信箱：2751801073@qq.com

读者交流群：218192911（办公之家）、99839857

郑重声明

本书对大量计算机及移动端的攻击行为进行了曝光，旨在帮助广大读者做好网络安全防范工作。

请广大读者注意：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是违法的！

CONTENTS

目录

第1章 黑客攻防入门

自从美国一项代号为“棱镜”的机密计划浮出水面，便引起人们对于黑客的更多关注。据美国中情局前职员爱德华·斯诺登爆料，美国国家安全局和联邦调查局从2007年起便开始在微软、谷歌、苹果、雅虎、Facebook、Skype、PalTalk、美国在线、YouTube等9家美国互联网公司进行数据挖掘工作，从音视频、图片、邮件、文档，以及连接信息分析个人的联系方式与行动。然而，这项计划不仅仅局限于美国国内，更是涉及全球范围，从而激起了人们对于黑客攻防技术的学习热情。下面通过本章的学习，快速地掌握黑客入门的基本知识。

学习要点

- 黑客入门的基础知识。
- 黑客常用的基本命令。
- 介绍常见的网络协议。
- 安装Vmware虚拟机及如何用Vmware创建虚拟环境、安装虚拟工具等。
- 系统编程语言C和C++运行环境codeblocks的安装和学习。

1.1 黑客是怎么形成的

1.1.1 什么是黑客

黑客通常是指对计算机科学、编程和设计方面具备高度理解能力的人，但是常常被理解为利用计算机网络技术搞破坏或者窃取信息的人 。

黑客一词在圈外或媒体上通常被定义为：专门入侵他人系统进行不法行为的计算机高手。不过，这类人士在 hacker 眼中是属于层次较低的 cracker（骇客）。如果黑客是炸弹制造专家，那么骇客就是恐怖分子。随着时代的发展，网络上出现了越来越多的骇客，他们只会入侵系统，使用扫描器到处乱扫，用 IP 炸弹炸目标主机，或者破解他人账号密码，替换、窃取他人隐私信息。

1.1.2 黑客的攻击方式

黑客攻击方式可分为非破坏性攻击和破坏性攻击两类。非破坏性攻击一般是为了扰乱系统的运行，并不盗窃系统资料，通常采用拒绝服务攻击或信息炸弹；破坏性攻击是以侵入他人计算机系统、盗窃系统保密信息、破坏目标系统的数据为目的。下面为大家介绍 5 种黑客常用的攻击手段。

1. 口令入侵

所谓口令入侵，就是指用一些软件解开已经得到但被人加密的口令文档，不过许多黑客已大量采用一种可以绕开或屏蔽口令保护的程序来完成这项工作。对于那些可以解开或屏蔽口令保护的程序通常被称为“Crack”。由于这些软件的广为流传，使得入侵计算机网络系统有时变得相当简单，一般不需要很深入了解系统的内部结构，是初级黑客常用的手段。

2. 木马入侵

说到特洛伊木马，只要知道这个故事的人就不难理解，它最典型的做法可能就是把一个能帮助黑客完成某一特定动作的程序依附在某一合法用户的正常程序中，这时合法用户的程序代码已被改变。一旦用户触发该程序，那么依附在内的黑客指令代码同时被激活，这些代码往往能完成黑客指定的任务。由于这种入侵法需要黑客有很好的编程经验，且要更改代码需要一定的权限，所以较难掌握。但正因为它的复杂性，一般的系统管理员很难发现。