Hackers Beware

黑客
——攻击透析与防范

[美] Eric Cole 著
苏 雷 等译

New Riders
電子工業出版社
Publishing House of Electronics Industry
www.phei.com.cn

黑　客

——攻击透析与防范

Hackers Beware

[美] Eric Cole　著

苏　雷　等译

電子工業出版社
Publishing House of Electronics Industry
北京 · Beijing

内容简介

本书全面、系统地介绍了关于网络安全技术的知识和相关问题。书中主要介绍了能够成功保护网络系统免受攻击的方法，并且对各种攻击的机理进行了全面的论述。本书的突出特点：全面跟踪了当前黑客攻击的关键技术和方法，针对不同对象和情况，提出了不同的防范策略，具有很强的实用性和时效性。本书结构合理、内容翔实，有助于训练安全方面的专门人才，使他们能够更好地对各种威胁做出正确的反应，使防范工作做在攻击者的前面。本书还可以为网络管理员、系统管理员在预防黑客方面提供有效的安全防范与管理策略。

图书在版编目（CIP）数据

黑客——攻击透析与防范/（美）科尔（Cole, E.）著；苏雷等译. -北京：电子工业出版社，2002.1
书名原文：Hackers Beware
ISBN 7-5053-7435-4

I. 黑... II. ①科... ②苏... 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（2001）第097835号

书　　名：**黑客——攻击透析与防范**
原 书 名：Hackers Beware
著　　者：[美] Eric Cole
译　　者：苏　雷　等
责任编辑：谭海平　杜　萌
排版制作：今日电子公司制作部
印 刷 者：北京天竺颖华印刷厂
出版发行：电子工业出版社　www.phei.com.cn
　　北京市海淀区万寿路173信箱　邮编：100036
经　　销：各地新华书店
开　　本：787 × 1092　1/16　　印张：37　字数：923千字
版　　次：2002年1月第1版　　2002年1月第1次印刷
书　　号：ISBN 7-5053-7435-4
　　TP·4287
定　　价：59.00元
著作权合同登记号　图字：01-2001-1463

译 者 序

在Internet高速发展的今天，黑客攻击越来越受到全社会的广泛关注，采用适当的安全技术成为保证网络系统正常运转的必要条件。但是由于各种原因，人们对黑客和网络安全存在很多误解。如今，任何计算机都不可能孤立存在，都需要通过网络相互通信。由于各种网络系统以及有关软件硬件系统的缺陷、各种系统管理方面的漏洞，导致了许多安全隐患，出现了许多严重的网络安全问题。

本书作者Eric Cole曾是美国中央情报局的雇员，现为SANS（系统管理、网络互联和安全研究机构）的发言人。他在网络安全方面拥有丰富的实践经验和扎实的理论基础。

网络安全并不是一句空话，需要实实在在的防范措施。但是在实施具体的措施之前，必须对黑客攻击进行充分的了解。本书介绍了关于黑客攻防和网络安全的知识，从黑客攻击的原因和方法入手，介绍了黑客在攻击前的准备，详细地讲述了攻击者使用的方法和工具。本书深入研究了黑客的心理并详细描述了攻击过程，对黑客攻击的每个阶段和各个方面，包括原理、功能、实施方法，都有实例加以说明。书中内容与各种漏洞和攻击原理以及攻击所使用的工具有关。本书还对Windows和UNIX操作系统所存在的主要漏洞，以及各种升级版本和补丁做了深入说明。更有价值的是，本书为系统安全性较脆弱或系统安全方面存在较多漏洞的各种网络提供了一系列的解决方法，并着重强调了根据SANS十大漏洞列表，修补主要的网络安全漏洞的必要性。

本书共20章，分别介绍了关于信息搜集、欺骗、会话劫持、拒绝服务攻击、缓冲区溢出攻击、口令安全等知识，同时结合实际介绍了口令破解和攻击实例，并讨论了黑客是如何保留访问权限和隐藏踪迹的。书中的案例非常典型，具有现实意义，相信每个读者都会受益匪浅。本书语言生动，内容深入浅出，讲解细致全面，是网络安全人员的必备参考书，也适合具备计算机基础知识的读者。本书的读者应具备有关网络、操作系统、TCP/IP、HTML、Perl或C语言等方面的基础知识。

本书由苏雷等翻译。参加翻译工作的还有：严静东、郭文明、贾振华、李冰、杨晓静、严炎、张立莉、王建东、范卫国、范永欣、章颖。参加审校工作的有：蔡开裕、曹介南、程健、窦勇、葛颖增、耿卫东、李恒年、李晓敏、刘宏伟、柳靖、彭秀文、石雄、孙宁、孙逊、陶菲、田兴彦、汪诗林、韦海亮、伍湘君、肖其英、袁静、徐钦桂、杨文、杨秀合、于贵桃、俞刚、余再祥、张永和、赵立军、郑军、周立、朱东升。该书在翻译和出版过程中得到了许多专家和同行的大力帮助和支持，在此谨向他们表示衷心的感谢，并向所有为本书中文版出版做出贡献的人们表示谢意。

由于本书内容新、翻译难度大、翻译时间非常紧迫，加之译者水平有限，错误和疏漏在所难免，恳请广大读者批评指正。

关于作者

Eric Cole 曾是美国中央情报局的雇员，现为SANS（系统管理、网络互联和安全研究机构）的高级发言人。他拥有纽约技术学院的理科学士学位和理科硕士学位，现在正在攻读网络安全博士学位，专攻入侵检测与隐蔽技术。Eric Cole在信息安全的诸多方面都有着广泛的经验，其中包括加密技术、隐蔽技术、入侵检测、NT安全、UNIX安全、TCP/IP和网络安全、Internet安全、路由器安全、安全评估、渗透试验、防火墙、安全的Web事务处理、电子商务、SSL、IPSEC以及信息战等。他是SANS的高级讲师，开设了多门课程，同时针对不同的课题做过系列演讲。Eric Cole还在纽约技术学院教学，同时担任乔治镇大学的助教。他还创办了Teligent公司，并兼任该公司安全部门的领导。

致　谢

感谢在本书写作过程中提供帮助与支持的New Riders出版公司，特别是Jeff Riley、Katherine Pendergast 和 Sean Monkhouse，他们是非常出色的发行人。

同时要感谢SANS。与 Alan Paller 和 Stephen Northcutt 一起工作令人愉快，他们给我提供了很大的帮助。在本书撰写的整个过程中，他们提出了很好的建议与支持。还要感谢SANS GIAC的学生们，他们提供了在实践中获得的极有价值的信息。

现在要感谢帮助我的所有朋友和家人。Tony Ventimiglia是一个同甘共苦的朋友，他给予了编辑方面的很大支持。Mathew Newfield提供了各方面的帮助。Jim Conley提供了编辑建议与指导。Gary Jackson是一位非常棒的朋友，给予了我不断的指导。Marc Maloof也同样给予了指导和帮助。

尤其是要感谢上帝赐予我的生命与和睦完美的家庭：Kerry Magee，大力支持我的妻子；Jackson，我可爱的儿子，给我每天的生活带来快乐；Ron和Caroline Cole、Mike和Ronnie Magee，给予我无数爱和支持的父母。还要感谢我的姐姐、姐夫、侄女、侄子：Cathy、Tim、Allison、Timmy和Brianna。

最后，为了所有我忘记提到名字的人，再一次感谢我的所有朋友、家人、同事以及在本书编写过程中给予我一切支持的所有人。

前　言

网络安全是一个流行的话题，有关这方面的书籍几乎不用介绍。大约十年以前，大多数人并不知道什么是Internet或电子邮件，再早一些时候，大多数家庭和办公室也没有计算机，一些人甚至在怀疑计算机与网络的用处。但是世界变化得太快了，当在写这篇简介的时候，感觉到网络世界的繁荣景象，就像是在迪斯尼世界中一样。十年前我们认为是科幻小说里才会有的东西现在不仅已变成了现实，而且已深入到了我们的生活之中。现在真正是计算机网络的时代了！

从功能的角度来讲，孤立的计算机是非常安全的。如果在家中放一台没有接入网络的计算机，那就不需要什么安全措施。可是现实中人们通过Internet把他们的计算机连接了起来，我们在互相信任的基础上建立了这个网。这里仅存在一个问题：人们之间并非完全互相信任。然而，在很多情况下，我们给所有用户完全的信息存取权。基于这一点，我们来追溯一下事情的起因。这其实是由于过去人们只关注于技术与功能，而并不担心安全问题，但事实上当前的安全问题已非常严重。

我还记得十年前在安全部门工作时的情景：人们都不愿搭理我，到处都给我白眼看。为什么会这样？因为人们还没有认识到安全工作的重要性，而是认为安全工作纯粹是在为根本不存在的威胁而浪费金钱。在那时，其他的技术和安全技术比起来，可以很容易地比较它们的效益。比如，扩展网络或安装新服务器可以加快访问速度、增加计算效率、提供更大的存储空间等。而安全技术却没有这些直接效益，它有的只是间接效益：数据和信息得到安全保障。一般情况下，在没有受到损失之前，人们是不会真正认识到安全的重要性的。只有当攻击者侵入了系统并盗走一千万美元的时候，人们才开始重视安全问题。想想看，如果他们一开始就在安全上投入的话，能省多少钱呢！

在越来越多的单位遭受损失的情况下，越来越多的单位认识到提前对安全投资的重要性。汽车保险就是这样，人们在买车的同时也买下了保险，只是为了防备万一车祸发生所带来的损失。我认识一些三十多年都没有发生过车祸的人，但是他们仍然购买保险。这是因为购买汽车保险可以降低出车祸时的损失，这已在人们心中形成了一种共识。同样的道理也适用于网络安全。不管您的公司是从事什么行当的，规模有多大，投资网络安全都是明智之举。

没有系统是安全的。任何接入Internet的系统都受到探测并有可能遭到侵入。我们可以做一些简单的实验来验证一下。可以用家中的直接接入或拨号接入Internet的计算机来做这个实验。购买或者从网上下载防火墙，这类软件工具有好几种，但Zone Alarm是一个免费版本，它可以从www.zonelabs.com下载。将这个防火墙安装在计算机系统上，接入Internet，48小时后会有吃惊的发现。通常在不到两天的时间内，系统会被探测到数次并可能被侵入。举个例子，当从Internet服务提供商（ISP）那里索要到一个IP后，接入网络，在不到30分钟的时间里就受到了5次探测。如果是家用计算机，没有域名，不受到太多关注，但还是被探测并受到攻击。对于公司而言，一定会受到更多攻击的。如果没有良好的防范措施，就会被非法攻入并遭受损失。

有一些公司曾对我说过，他们的系统从来都没有受到过攻击。这些话肯定是不对的。事实上，应该是他们从来都没有检测到攻击。眼不见心不烦并不能解决问题，清楚并能针对自己系

统进行恰当的防范措施是非常关键的。本书就是要介绍黑客们在干什么以及他们所用的工具和技术。通过本书，可以从准确的角度对系统做出更好的防范。

应该明确，成功的防范必须建立在对攻击充分了解的基础之上，这正是本书的目的：介绍黑客攻击与破坏的技术、方法以及工具，让人们利用这些知识建立更安全的网络。安全防范不是一句空话，必须了解威胁是什么。在这个领域只有知识是最有力量的。

本书就是介绍黑客攻击的内幕以及如何防范黑客的关键。保护网络安全是一次没有终点的旅行，但就我的经验来看，它也是一次非常令人愉快而且回报相当大的旅行。快让我们开始在网络安全世界中的美妙旅途吧！

目　录