<<黑客攻防实战编程>>

图书基本信息

书名：<<黑客攻防实战编程>>

13位ISBN编号：9787121085376

10位ISBN编号：7121085372

出版时间：2009-6

出版时间：电子工业出版社

作者：邓吉

页数：362

字数：436000

前言

《黑客攻防实战入门》、《黑客攻防实战详解》和《黑客攻防实战进阶》这3本书自面世以来，得到了广大读者的肯定与好评。
其销量一直排在同类书籍的前列，笔者在此深表感谢。
与此同时，应广大读者的要求，笔者针对当前黑客编程领域的热点及难点问题，撰写了这本《黑客攻防实战编程》一书。
本书一如既往地保持着前3本书的“授之以鱼，不如授之以渔”的风格，向读者介绍黑客入侵及防御相关编程技术的思考方法和思维方式，而不是单单介绍编程语法。
本书是笔者通过多年的研究与实践，在把握国内外安全领域研究的热点及难点的基础之上，进行归纳总结所完成的一本黑客编程入门及提高书籍，这一点是本书区别于其他同类书籍的根本之处。
关于黑客　　长期以来，由于诸多方面的因素，“黑客”这个字眼变得十分敏感。
不同的人群对黑客也存在不同的理解，甚至没有人愿意承认自己是黑客。
有些人认为，黑客是一群狂热的技术爱好者，他们无限度地追求技术的完美；有些人认为，黑客只是一群拥有技术，但思想简单的毛头小伙子；还有些人认为黑客是不应该存在的，他们是网络的破坏者。
这里，我们没有必要对这个问题争论不休，也无须为黑客加上一个标准的定义，但从客观存在的事实来看，黑客这类群体往往存在以下共同点。
（1）强烈的技术渴望与完美主义：驱动他们成长的是对技术的无限渴望，获得技术的提高才是他们最终的任务。
（2）强烈的责任感：只有强烈的责任感才能使他们不会走向歧途，责任感告诉他们不要在任何媒体上公布成功入侵的服务器；不要对其入侵的服务器进行任何破坏；在发现系统漏洞后要立即通知官方对该漏洞采取必要的修补措施。
在官方补丁没有公布之前，绝对不要大范围地公开漏洞利用代码。
一方面，黑客入侵可能造成网络的暂时瘫痪；另一方面，黑客也是整个网络的建设者，他们不知疲倦地寻找网络大厦的缺陷，使得网络大厦的根基更加稳固。
为什么写作本书　　不容乐观的事实是，一部分人歪曲了黑客的本质，被不良动机所驱使而进行入侵活动，威胁网络的健康发展。
对于我国来说，形势尤为严峻。
我国信息化建设迟于美国等发达国家，信息安全技术水平也相对落后。
在几次黑客大战中，国内网站的弱口令及漏洞比比皆是。
这种现状实在令人担忧，值得深思和反省，从中也可以看出传统的计算机网络教学层次是远远不够的。
可能出于安全等其他角度的考虑，传统教学往往只注重表面上的应用，而避开一些敏感的技术。
设想一下，如果一个网站的管理员只学会架构网站，却不关心如何入侵自己的网站，那么如何对自己网站的缺陷了如指掌？
如何能够及时地获知最新漏洞的描述而提前做好抵御？
如果以上都做不到，那就更不要谈日常的系统更新、维护和打补丁了。
然而国内精通入侵的网管又有多少呢？
长期以来，国内网管的潜意识里都认为“入侵”是个不光彩的勾当，甚至嗤之以鼻。
随着信息化程度越来越高，信息技术与生活的联系越来越紧密，可以上网的电子设备逐年增加，电脑、PDA、手机，甚至家电。
可以想像10年后，如果不了解入侵者的手段来采取必要的防御措施，将要被入侵的设备不会仅仅限于电脑，也许还包括手机、家电和汽车等。
因此在信息技术如此发达，沟通方式日益丰富和复杂的今天，我们不仅要学会如何正确使用网络，而且还需要学会如何防御自己的网络被他人入侵，这也正是笔者写作本书的初衷。
本书主要内容　　作为《黑客攻防实战入门》、《黑客攻防实战详解》和《黑客攻防实战进阶》

的提高篇，本书以黑客“攻”、“防”的视角，针对目前国内外安全研究的热点和难点问题进行研究，涵盖了Web入侵脚本、病毒、木马、网马、加密解密、Shellcode、漏洞溢出渗透，以及漏洞挖掘等相关领域的程序开发研究。

本书分为内容独立的7章，读者可以根据实际需求有选择跳跃式阅读，各章的主要内容如下。

第1章“Web入侵脚本编程”从服务器搭建开始，介绍目前网络上最为猖獗的“SQL注入”和“跨站脚本攻击”入侵手段、原理与编程技术，以及防护手段。

第2章“病毒原理及代码解析”在总结计算机病毒发展历史、病毒种类及病毒命名方式之后，详细地介绍计算机病毒原理，并对病毒源代码进行了全面的剖析。

第3章“木马网马程序分析”针对木马及网马的源代码进行解析、总结了其工作原理、启动方式、隐藏与防杀等相关技术。

第4章“软件加密与解密”介绍序列号保护、软件加密狗、时间限制及Key文件保护等目前常见软件的加密方法，并分析注册机等软件的解密原理，以及跟踪调试与反跟踪调试技术。

第5章“shellcode原理与编写”介绍了栈溢出、堆溢出等程序溢出原理，分析了PE文件结构，以及如何针对已知漏洞编写Shellcode。

第6章“漏洞溢出程序分析与设计”详细介绍了缓冲区溢出原理、类Unix、Windows及远程Windows程序溢出方法等渗透方法，并介绍一款自动化渗透测试工具Metasploit及其使用方法。

第7章“漏洞挖掘与Fuzzing程序设计”介绍一种行之有效的自动化漏洞挖掘技术“Fuzzing”，进而介绍如何挖掘已知系统中所存在的漏洞。

另外，本书中所使用的源代码及动画教程等相关资源下载，链接地址为http://www.broadview.com.cn。

本书的姊妹书籍　　本书的姊妹书籍有《黑客攻防实战入门(第2版)》、《黑客攻防实战详解》和《黑客攻防实战进阶》3本，在本书推出之后，这4本书便形成了一个由浅入深完整的知识体系。几乎涵盖了黑客安全领域由入门到专家所必需掌握的所有的知识与技术，以供不同层次的读者学习。

（1）《黑客攻防实战入门》：踏入网络安全之门，初窥黑客攻防实战技巧。

（2）《黑客攻防实战详解》：透析网络安全内幕，详解黑客攻防体系。

（3）《黑客攻防实战进阶》：深入网络安全技术，进阶黑客攻防专家。

（4）《黑客攻防实战编程》：把握网络安全方向，实战黑客攻防编程。

致谢　　感谢张毅编辑在我还是学生时代时就接受了我的《黑客攻防实战入门》样稿，才使得这么多年我都有机会和信心将自己的经验通过电子工业出版社分享给广大读者朋友。

感谢毕宁编辑长年来的指导与支持，并推荐给我大量的朋友与学习机会。才使得我能够陆续撰写《黑客攻防实战入门（第2版）》、《黑客攻防实战详解》、《黑客攻防实战进阶》和《黑客攻防实战编程》这4本书。

感谢孙学瑛老师和黄爱萍助理的指导，以及为本书的出版所付出辛勤劳动的所有朋友。

感谢qixu.liu在技术方面给与我的支持。

感谢长期以来支持我的读者朋友和网友们。

需要声明的是，本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任。

本书的目的在于最大限度地唤起大家的网络安全意识，正视我们的网络世界所面临的一场危机并采取相应的行动。

<<黑客攻防实战编程>>

内容概要

《黑客攻防实战编程》一书作为《黑客攻防实战入门》、《黑客攻防实战详解》和《黑客攻防实战进阶》的提高篇，仍然以黑客“攻”、“防”的视角，针对目前国内外安全研究的热点和难点问题进行研究，内容涵盖了Web入侵脚本、病毒、木马、网马、加密解密、Shellcode、漏洞溢出渗透、以及漏洞挖掘等相关领域的程序开发研究。
本书适合信息安全领域研究人员、机构、网管和那些对网络感兴趣的在校学生作为参考及教学之用，也适合杀毒软件、木马查杀软件等相关网络安全工具的开发人员作为参考之用。

<<黑客攻防实战编程>>

书籍目录

编辑推荐

在信息技术如此发达，沟通方式日益丰富和复杂的今天，我们不仅要学会如何正确地使用网络，而且还需要学会如何防御自己的网络被他人入侵，这也正是《黑客攻防实战编程》的写作初衷。

《黑客攻防实战编程》是笔者通过多年的研究与实践，在把握国内外安全领域研究的热点及难点的基础之上，进行归纳总结所完成的一本黑客攻防编程入门及提高书籍：

第1章“Web入侵脚本编程”从服务器搭建开始，介绍目前网络上最为猖獗的“SQI一注入”和“跨站脚本攻击”入侵手段、原理与编程技术，以及防护手段。

第2章“病毒原理及代码解析”在总结计算机病毒发展历史、病毒种类及病毒命名方式之后，详细地介绍计算机病毒原理，并对病毒源代码进行了全面的剖析。

第3章“木马网马程序分析”针对木马及网马的源代码进行解析、总结了其工作原理、启动方式、隐藏与防杀等相关技术。

第4章“软件加密与解密”介绍序列号保护、软件加密狗、时间限制及Key文件保护等目前常见软件的加密方法，并分析注册机等软件的解密原理，以及跟踪调试与反跟踪调试技术。

第5章“shellcode原理与编写”介绍了栈溢出、堆溢出等程序溢出原理，分析了PE文件结构，以及如何针对已知漏洞编写Srlellcode。

第6章“漏洞溢出程序分析与设计”详细介绍了缓冲区溢出原理、类unix、Windows及远程Windows程序溢出方法等渗透方法，并介绍一款自动化渗透测试工具Metasploit及其使用方法。

第7章“漏洞挖掘与Fuzzing程序设计”介绍一种行之有效的自动化漏洞挖掘技术“Fuzzing”，进而介绍如何挖掘已知系统中所存在的漏洞。

另外，《黑客攻防实战编程》中所使用的源代码及动画教程等相关资源下载，链接地址为：

版权说明