《黑客攻防技术宝典》

图书基本信息

书名：《黑客攻防技术宝典》

13位ISBN编号：9787115328489

10位ISBN编号：711532848X

出版时间：2013-9

出版社：人民邮电出版社

作者：[美]Charlie Miller,[美]Dionysus Blazakis,[美]Dino Dai Zovi,[美]Stefan Esser,[美]Vincenzo Iozzo,[美]Ralf-Philipp Weinmann

页数：320

译者：傅尔也

《黑客攻防技术宝典》

内容概要

安全始终是计算机和互联网领域最重要的话题。进入移动互联网时代，移动平台和设备的安全问题更加突出。iOS系统凭借其在移动市场的占有率拥有着举足轻重的地位。虽然iOS系统向来以安全著称，但由其自身漏洞而引发的威胁同样一直存在。
《黑客攻防技术宝典：iOS实战篇》由美国国家安全局全球网络漏洞攻击分析师、连续4年Pwn2Own黑客竞赛大奖得主Charlie Miller领衔，6位业内顶级专家合力打造，全面深入介绍了iOS的工作原理、安全架构、安全风险，揭秘了iOS越狱工作原理，探讨了加密、代码签名、内存保护、沙盒机制、iPhone模糊测试、漏洞攻击程序、ROP有效载荷、基带攻击等内容，为深入理解和保护iOS设备提供了足够的知识与工具，是学习iOS设备工作原理、理解越狱和破解、开展iOS漏洞研究的重量级专著。
本书作为国内第一本全面介绍iOS漏洞及攻防的专著，作者阵容空前豪华，内容权威性毋庸置疑。Charlie Miller曾在美国国家安全局担任全球网络漏洞攻击分析师5年，并连续4届摘得Pwn2Own黑客竞赛桂冠。Dionysus Blazakis擅长漏洞攻击缓解技术，2010年赢得了Pwnie Award最具创新研究奖。Dino Dai Zovi是Trail of Bits联合创始人和首席技术官，有十余年信息安全领域从业经验，出版过两部信息安全专著。Vincenzo Iozzo现任BlackHat和Shakacon安全会议评审委员会委员，因2010年和2011年连续两届获得Pwn2Own比赛大奖在信息安全领域名声大振。Stefan Esser是业界知名的PHP安全问题专家，是从原厂XBOX的硬盘上直接引导Linux成功的第一人。Ralf-Philipp Weinmann作为德国达姆施塔特工业大学密码学博士、卢森堡大学博士后研究员，对密码学、移动设备安全等都有深入研究。
本书适合想了解iOS设备工作原理的人，适合对越狱和破解感兴趣的人，适合关注iOS应用及数据安全的开发人员，适合公司技术管理人员（他们需要了解如何保障iOS设备安全），还适合从事iOS漏洞研究的安全研究人员。

《黑客攻防技术宝典》

作者简介

Charlie Miller
Accuvant Labs首席研究顾问，曾在美国国家安全局担任全球网络漏洞攻击分析师5年，连续4年赢得CanSecWest Pwn2Own黑客大赛。他发现了iPhone与G1安卓手机第一个公开的远程漏洞，通过短信对iPhone进行漏洞攻击并发现了可以让恶意软件进入iOS的代码签名机制缺陷。作为圣母大学博士的他还与人合著了The Mac Hacker's Handbook和Fuzzing for Software Security Testing and Quality Assurance两本信息安全类图书。
Dionysus Blazakis
程序员和安全研究人员，擅长漏洞攻击缓解技术，经常在安全会议上发表有关漏洞攻击缓解技术、绕过缓解技术和寻找漏洞的新方法等主题演讲，因利用即时编译器绕过数据执行保护的技术赢得了2010年Pwnie Award最具创新研究奖。另外，他与Charlie Miller为参加2011年Pwn2Own大赛开发的iOS漏洞攻击程序赢得了iPhone漏洞攻击比赛的大奖。
Dino Dai Zovi
Trail of Bits联合创始人和首席技术官，有十余年信息安全领域从业经验，
做过红队（red teaming，又称“伦理黑客”）、渗透测试、软件安全、信息安全管理和网络安全研究与开发等多种工作。Dino是信息安全会议的常客，在DEFCON、BlackHat和CanSecWest等世界知名的信息安全会议上发表过对内存损坏利用技术、802.11无线客户端攻击和英特尔VT-x虚拟化rootkit程序等课题的独立研究成果。他还是The Mac Hacker's Handbook和The Art of Software Security Testing的合著者。
Vincenzo Iozzo
Tiqad srl安全研究人员，BlackHat和Shakacon安全会议评审委员会成员，常在BlackHat和CanSecWest等信息安全会议上发表演讲。他与人合作为BlackBerryOS和iPhoneOS编写了漏洞攻击程序，因2010年和2011年连续两届获得Pwn2Own比赛大奖在信息安全领域名声大振。
Stefan Esser
因在PHP安全方面的造诣为人熟知，2002年成为PHP核心开发者以来主要关注PHP和PHP应用程序漏洞的研究，早期发表过很多关于CVS、Samba、OpenBSD或Internet Explorer等软件中漏洞的报告。2003年他利用了XBOX字体加载器中存在的缓冲区溢出漏洞，成为从原厂XBOX的硬盘上直接引导Linux成功的第一人；2004年成立Hardened-PHP项目，旨在开发更安全的PHP，也就是Hardened-PHP（2006年融入Suhosin PHP安全系统）；2007年与人合办德国Web应用开发公司SektionEins GmbH并负责研发工作；2010年起积极研究iOS安全问题，并在2011年提供了一个用于越狱的漏洞攻击程序（曾在苹果多次更新后幸存下来）。
Ralf-Philipp Weinmann
德国达姆施塔特工业大学密码学博士、卢森堡大学博士后研究员。他在信息安全方面的研究方向众多，涉及密码学、移动设备安全等很多主题。让他声名远播的事迹包括参与让WEP破解剧烈提速的项目、分析苹果的FileVault加密、擅长逆向工程技术、攻破DECT中的专属加密算法，以及成功通过智能手机的Web浏览器（Pwn2Own）和GSM协议栈进行渗透攻击。

《黑客攻防技术宝典》

书籍目录

目 录

《黑客攻防技术宝典》

精彩短评

1、强
2、译得烂死了。
3、图书馆
4、iOS上的黑客书，不过没开发过什么应用读起来有点吃力
5、4/13，拿去图书漂流了
6、任何的安全 接触到物理层面都没有安全科言 随着互联网的发生将有可能通过互联网来接触物理层面；
7、内力不够，曰，弃之。

《黑客攻防技术宝典》

精彩书评

1、1、翻译质量着实不敢恭维，很多是直译的。由于英文经常习惯用长句，如果直译成中文就会变得很绕口，完全不符合国人的表达思维。英译中就该把长句变短句，否则单纯从语义表面上看都相当费劲，更不用说技术层面了。比如下面这句：“ 其它代码可能调用xx以调用xx函数中的函数，如果你调用原始xx，就会因为副本xx未更新造成一致性问题 ”，真的很绕口。2、书中不少专业术语翻译不到位，比如"return-into-libc"利用技术居然被翻译成“ 返回libc中 ”，还有其它不少地方也是如此，表达上不过明确，可见译者对软件安全技术的不熟悉。3、书中有少表达不明确的地方，还有笔误，这种即使是非技术人员应该也是可以看出来的，说明编辑审稿不严格，双方均有责任。
2、本书看了三分之一，对里面介绍的一些技术，文字意思到能理解，但一些基础代码和基础函数就比较难以理解！边看边百度搜索一些专业术语，进度挺慢！里面有个专业术语，一直没怎么弄明白，“ ROP有效载荷 ”这个东西，不知道是什么，百度上说的是“ 信息数据元什么的 ”，还是不理解T_T

《黑客攻防技术宝典》

版权说明