<<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：9787115217967

10位ISBN编号：7115217963

出版时间：2010-1

出版时间：人民邮电出版社

作者：Chris Anley,John Heasman,Felix Linder,Gerardo Richarte

页数：545

字数：826000

译者：罗爱国,郑艳杰

前言

“如果术语的含义总是变来变去，不仅会导致原本不相干的推理发生混淆，就连既定的前提和结论也会频繁地被颠倒。
”　　——摘自艾达·奥古斯塔在Sketch of The Analytical Engine一书（1842年）中所做的注释　　本书第1版主要介绍了怎样发现和利用安全漏洞，第2版仍然紧紧围绕这一主题展开。
如果你是一位技术娴熟的网络审计员、软件开发人员或系统管理员，如果你想弄明白如何发现和利用最底层的bug，这本书将是你最好的选择。
　　那么本书究竟会讲些什么呢？
前面的内容或多或少概括了一些。
本书主要关注任意的代码执行漏洞，攻击者借这些漏洞在目标机器上运行他们的代码。
这种情况发生时，通常程序会把数据解释成自身的一部分，例如，攻击者利用此类漏洞可以把HTTP的Host首部变成返回地址，把Email地址的一部分变成函数指针，等等。
程序在执行这些数据之后，结果通常都是灾难性的。
现代处理器、操作系统以及编译器的架构是此类问题产生的根源，正如艾达所言，“操作的记号通常也是操作结果的记号”。
当然，她讨论的是数学中的难点：数字5可能意味着“5次方”，也可能意味着“第5个元素”，但基本的思想是一致的。
如果你混淆了代码和数据，就会陷入困境。
因此，本书就来讨论代码和数据，以及混淆两者可能会带来的后果。
　　自本书第1版于2004年面世以来，安全领域变得更加复杂了，世界也发生了很大的变化。
一方面，编译器和操作系统普遍内置了防护措施，用于防范本书重点讨论的各种漏洞——当然，这些措施远远还谈不上尽善尽美。
另一方面，尚无迹象表明任意代码执行漏洞的“供应”在不久的将来会难以为继，更何况查找这些漏洞的方法仍在不断花样翻新。
如果你访问美国国家漏洞数据库网站（nvd.nist.gov），单击statistics，选择buffer overflow，就会发现缓冲区溢出的数量逐年增加。

<<黑客攻防技术宝典>>

内容概要

本书由世界顶级安全专家亲自执笔，详细阐述了系统安全、应用程序安全、软件破解、加密解密等安全领域的核心问题，并用大量的实例说明如何检查Windows、Linux、Solaris等流行操作系统中的安全漏洞和Oracle等数据库中的安全隐患。

本书适用于所有计算机安全领域的技术人员和管理人员以及对计算机安全感兴趣的爱好者。

作者简介

Chris Anley，世界知名系统安全专家。
具有各种操作系统漏洞挖掘的丰富经验。
Next Generation安全软件公司创始人、总监。
John Heasman，世界知名安全专家，尤其擅长于企业级软件安全攻防技术。
著有多篇安全方面的颇有影响力的论文。
现任Next Generation安全软件公司研发总监。
FeIix“ FX ”Linder，世界知名安全专家。
具有近20年的计算机安全领域工作经验，熟悉各种操作系统特性。
目前领导着德国著名安全技术咨询公司SABRE Labs。
Gerardo Richarte，著名安全技术专家。
精通漏洞挖掘和逆向工程。
他还参与开发了著名的SqueakNOS项目。
现为Core安全技术公司技术骨干。

<<黑客攻防技术宝典>>

书籍目录

章节摘录

为了理解本书的大部分内容，我们还必须掌握汇编语言，尤其是IA32上的汇编语言。
原因有三：一是本书中所举的例子大部分都是用IA32汇编语言编写的；二是在寻找bug的过程中，我们需要阅读并理解汇编指令；三是在大多数利用安全漏洞的过程中，我们需要自己编写（或修改已存在的）汇编程序。

除IA32外，熟知其他的硬件体系结构也很重要（只是破解起来稍微有些难度），因此，我们在书中用了几章介绍怎样在非IA32平台上发现和利用漏洞。
我们建议：如果你打算在某种硬件平台上研究安全问题，那么一定要牢固掌握汇编语言（尤其是你选择的硬件结构体系的汇编语言），这对你的帮助将非常大。

如果在此之前，你没有接触过汇编语言，那么我建议你先从数字系统（特别是十六进制）、数据大小、数值符号表示等内容学起，这些内容在大多数大学计算机体系架构教材里都可以找到。

寄存器　　要想发现并利用漏洞，一定要熟悉IA32寄存器以及怎样用汇编指令操作它们。
可以用汇编指令访问（读、写）寄存器。

寄存器是存储器，考虑到性能的因素，通常直接把寄存器和总线连在一起。
现代计算机系统在执行操作时要使用寄存器，一般用汇编指令来操作寄存器。
从应用的角度可以把寄存器分为4类：　　通用寄存器　　段寄存器　　控制寄存器　　其他寄存器

媒体关注与评论

“黑客圣经！
如果你想了解系统安全知识并成为一名黑客高手，此书必读！
”——美国《计算机周刊》 “这几位作者都是我景仰的安全技术高手。
能分享到他们一些鲜为人知的安全攻防技巧，幸甚。
”——Amazon.com

编辑推荐

操作系统是连接计算机硬件与上层软件及用户的桥梁，其安全性至关重要。
知己知彼.方能百战不殆，用户只有了解了系统中存在的可被利用的漏洞和攻击者所采用的攻击方法。才能更有效地确保系统安全。

《黑客攻防技术宝典：系统实战篇(第2版)》由4位世界顶级安全技术大师联袂打造.全面介绍了操作系统的安全问题。
从最基本的栈、堆、内存布局等方面着手，逐渐深入到操作系统的各个层面。
重点阐述如何发现和防范系统的安全漏洞。
全书内容均来自作者一线实战经验总结，强调动手实践和探索的重要性，自始至终体现了钻研无止境的黑客精神。

跟世界顶级安全技术大师学习黑客攻防技术　　全面分析系统安全漏洞　　大量实例和代码片段

版权说明