0day安全：软件漏洞分析技术（第2版）

安全技术大系

0day安全：软件漏洞分析技术（第2版）

王清主编

ISBN978-7-121-13396-1

2011年6月出版

定价：85.00元

16开

780页

内 容 简 介

本书分为5篇33章，系统、全面地介绍了Windows平台缓冲区溢出漏洞的分析、检测与防护。第一篇为漏洞exploit的基础理论和初级技术，可以引领读者迅速入门；第二篇在第一篇的基础上，结合国内外相关研究者的前沿成果，对漏洞技术从攻、防两个方面进行总结；第三篇站在安全测试者的角度，讨论了几类常用软件的漏洞挖掘方法与思路；第四篇则填补了本类书籍在Windows内核安全及相关攻防知识这个神秘领域的技术空白；第五篇以大量的0 day案例分析，来帮助读者理解前四篇的各类思想方法。

本书可作为网络安全从业人员、黑客技术发烧友的参考指南，也可作为网络安全专业的研究生或本科生的指导用书。

自 序

虽然事隔多年，我仍然清晰记得自己被“冲击波”愚弄的场景——2003年夏的那个晚上，自己像往常一样打开实验室的计算机，一边嘲笑着旁边同学因为不装防火墙而被提示系统将在一分钟内关机，一边非常讽刺地在自己的计算机上发现了同样的提示对话框。正是这个闻名世界的“框框”坚定了我投身网络安全研究的信念，而漏洞分析与利用正是这个领域的灵魂所在。

漏洞分析与利用的过程是充满艺术感的。想象一下，剥掉Windows中那些经过层层封装的神秘的对话框“外衣”，面对着浩如烟海的二进制机器码，跋涉于内存中不知所云的海量数据，在没有任何技术文档可以参考的情况下，进行反汇编并调试，把握函数调用和参数传递的细节，猜测程序的设计思路，设置巧妙的断点并精确定位到几行有逻辑缺陷的代码，分析研究怎么去触发这个逻辑漏洞，最后编写出天才的渗透代码，从而得到系统的控制权……这些分析过程的每一个环节无不散发着充满智慧的艺术美感！这种技术不同于其他计算机技术，它的进入门槛很高，需要拥有丰富的计算机底层知识、精湛的软件调试技术、非凡的逻辑分析能力，还要加上一点点创造性的思维和可遇而不可求的运气。

在无数个钻研这些技术的夜里，我深深地感觉到国内的漏洞分析资料和文献是多么匮乏。为了真正搞清楚蠕虫病毒是怎样利用Windows漏洞精确淹没EIP寄存器并获得进程控制权，我仍然记得自己不得不游走于各种论坛收集高手们零散手稿时的情形。那时的我多么希望能有一本教材式的书籍，让我读了之后比较全面、系统地了解这个领域。

我想，在同样漆黑的夜里，肯定还有无数朋友和我从前一样，满腔热情地想学习这门技术而又困惑于无从下手。正是这种“请缨无处，剑吼西风”的感觉，激励着我把自己钻研的心血凝结成一本教程，希望这样一本教程可以帮助喜欢网络安全的朋友们在学习时绕开我曾走过的弯路。

再版序

距离《0day安全：软件漏洞分析技术》的出版已有3年，接到再版约稿的时候我着实有一番感慨，也有着太多的内容想与大家分享。在这3年里，我经历了从一个初出象牙塔的少年到安全分析员的演变。期间我参加了若干次安全事件的应急响应、在若干个安全峰会上做过漏洞技术的演讲、完成了无数次的渗透测试、也有幸见证了先行者们在Windows平台上进行的最为精彩的几场较量……

为了在再版中更加完美地总结这精彩的几年，我特意邀请了几位和我意气相投的兄弟加入编写团队，他们是：

熟悉Windows内核机制的张东辉（Shineast，负责编写内核安全部分）；

精通Windows各类保护机制的周浩（Zihan，负责编写高级溢出部分）；

黑客防线的知名撰稿人、漏洞挖掘专家王继刚（爱无言，负责编写漏洞挖掘部分）；

文件格式解析专家赵双（Dflower，负责编写文件型漏洞测试部分）；

资深病毒分析员蔡山枫（Beanniecai，编写样本分析和案例分析的部分章节）。

团队的力量大大增强了再版内容的广度和深度。再版中新增了大量前沿知识和案例分析，囊括了Windows平台高级溢出技巧、手机平台的溢出基础、内核攻防、漏洞挖掘与安全测试、大量的0day分析案例等。此外我们还对Windows平台中高级防护技巧和部分经典案例的分析等内容进行了修订和勘误。第一版中关于基础溢出的知识也得以保留，在经过重新编排和浓缩后，放置在再版的第一篇供入门者学习。

在计算机工业向模块化、封装化、架构化发展的过程中，人们更加倾向于把时间和精力用于那些敏捷开发的高级工具上。走进大学的计算机系你可以发现J2EE与.NET的书籍随处可见，但是却没有几个学生能在二进制级别把计算机体系结构讲清。甚至在某些网络安全学院里，能把蠕虫入侵的原理刨根问底彻底、弄清的也是凤毛麟角，非好奇心不盛也，乃道之不传也久矣。在信息安全这条道路上行走，需要“男儿何不带吴钩，收取关山五十州”的豪情，需要“臣心一片磁针石，不指南方不肯休”的毅力，需要“壁立千仞，无欲则刚”的情怀……我等立书只为布道交友，最大的收益莫过于帮助还在彷徨如何入门的朋友迈过那条门槛，通过此书结交更多的同道中人。

前 言

关于安全技术人才

国内外对网络安全技术人才的需求量很大，精通缓冲区溢出攻击的安全专家可以在大型软件公司轻易地获得高薪的安全咨询职位。

信息安全技术是一个对技术性要求极高的领域，除了扎实的计算机理论基础外，更重要的是优秀的动手实践能力。在我看来，不懂二进制数据就无从谈起安全技术。

国内近年来对网络安全的重视程度正在逐渐增加，许多高校相继成立了“信息安全学院”或者设立“网络安全专业”。科班出身的学生往往具有扎实的理论基础，他们通晓密码学知识、知道PKI体系架构，但要谈到如何真刀实枪地分析病毒样本、如何拿掉PE上复杂的保护壳、如何在二进制文件中定位漏洞、如何对软件实施有效的攻击测试……能够做到的人并不多。

虽然每年有大量的网络安全技术人才从高校涌入人力市场，真正能够满足用人单位需求的却寥寥无几。捧着书本去做应急响应和风险评估是滥竽充数的作法，社会需要的是能够为客户切实解决安全风险的技术精英，而不是满腹教条的阔论者。

我所认识的很多资深安全专家都并非科班出身，他们有的学医、有的学文、有的根本没有学历和文凭，但他们却技术精湛，充满自信。

这个行业属于有兴趣、够执著的人，属于为了梦想能够不懈努力的意志坚定者。

关于“Impossible”与“I’m possible”

从拼写上看，“Impossible”与“I’mpossible”仅仅相差一个用于缩写的撇号（apostrophe）。学完本书之后，您会发现将“不可能（Impossible）”变为“可能（I’mpossible）”的“关键（keypoint）”往往就是那么简单的几个字节，本书将要讨论的就是在什么位置画上这一撇！

从语法上看，“Impossible”是一个单词，属于数据的范畴；“I’mpossible”是一个句子，含有动词（算符），可以看成是代码的范畴。学完本书之后，您会明白现代攻击技术的精髓就是混淆数据和代码的界限，让系统错误地把数据当作代码去执行。

从意义上看，Tobe the apostrophe which changed “Impossible” into “I’m possible” 代表着人类挑战自我的精神，代表着对理想执著的追求，代表着对事业全情的投入，代表着敢于直面惨淡人生的豪情……而这一切正好是黑客精神的完美诠释——还记得在电影《SwordFish（剑鱼行动）》中，Stan在那台酷毙的计算机前坚定地说：“Nothingis impossible”，然后开始在使用Vernam加密算法和512位密钥加密的网络上，挑战蠕虫的经典镜头吗？

于是我在以前所发表过的所有文章和代码中都加入了这个句子。尽管我的英语老师和不少外国朋友提醒我，说这个句子带有强烈的“Chinglish”味道，甚至会引起NativeSpeaker的误解，然而我最终还是决定把它写进书里。

虽然我不是莎士比亚那样的文豪，可以创造语言，发明修辞，用文字撞击人们的心灵，但这句“Chinglish”的确能把我所要表达的含义精确地传递给中国人，这已足够。

关于本书

通常情况下，利用缓冲区溢出漏洞需要深入了解计算机系统，精通汇编语言乃至二进制的机器代码，这足以使大多数技术爱好者望而却步。

随着时间的推移，缓冲区溢出攻击在漏洞的挖掘、分析、调试、利用等环节上已经形成了一套完整的体系。伴随着调试技术和逆向工程的发展，Windows平台下涌现出的众多功能强大的debug工具和反汇编分析软件逐渐让二进制世界和操作系统变得不再神秘，这有力地推动了Windows平台下缓冲区溢出的研究。除此以外，近年来甚至出现了基于架构（FrameWork）的漏洞利用程序开发平台，让这项技术的进入门槛大大降低，使得原本高不可攀的黑客技术变得不再遥不可及。

遗憾的是，与国外飞速发展的高级黑客技术相比，目前国内还没有系统介绍Windows平台下缓冲区溢出漏洞利用技术的专业书籍，而且相关的中文文献资料也非常匮乏。

本书将系统全面地介绍Windows平台软件缓冲区溢出漏洞的发现、检测、分析和利用等方面的知识。

为了保证这些技术能够被读者轻松理解并掌握，本书在叙述中尽量避免枯燥乏味的大段理论阐述和代码粘贴。概念只有在实践中运用后才能真正被掌握，这是我多年来求学生涯的深刻体会。书中所有概念和方法都会在紧随其后的调试实验中被再次解释，实验和案例是本书的精髓所在。从为了阐述概念而精心自制的漏洞程序调试实验到现实中已经造成很大影响的著名漏洞分析，每一个调试实验都有着不同的技术侧重点，每一个漏洞利用都有自己的独到之处。

我将带领您一步一步地完成调试的每一步，并在这个过程中逐步解释漏洞分析思路。不管您是网络安全从业人员、黑客技术发烧友、网络安全专业的研究生或本科生，如果您能够完成这些分析实验，相信您的软件调试技术、对操作系统底层的理解等计算机能力一定会得到一次质的飞跃，并能够对安全技术有一个比较深入的认识。

关于本书源代码及相关文档

本书中调试实验所涉及的所有源代码和PE文件都可从看雪论坛相关版面下载http://zeroday.pediy.com。

这些代码都经过了仔细调试，如在使用中发现问题，请查看实验指导中对实验环境的要求。个别攻击实验的代码可能会被部分杀毒软件鉴定为存在风险的文件，请您调试前详细阅读实验说明。

关于对读者的要求

虽然溢出技术经常涉及汇编语言，但本书并不要求读者一定具备汇编语言的开发能力。所用到的指令和寄存器在相关的章节都有额外介绍，只要您有C语言基础就能消化本书的绝大部分内容。

我并不推荐在阅读本书之前先去系统的学习汇编知识和逆向知识，枯燥的寻址方式和指令介绍很容易让人失去学习的兴趣。本书将带您迅速跨过漏洞分析与利用技术的进入门槛。即使您并不懂汇编与二进制也能完成书中的调试实验，并获得一定的乐趣。当然，在您达到一定水平想进一步提高时，补习逆向知识和汇编语言将是绝对必要的。

本书适合的读者群体包括：

l 安全技术工作者　本书比较全面、系统地收录了Windows平台下缓冲区溢出攻击所涉及的各种方法，将会是一本不错的技术字典。

l 信息安全理论研究者　本书中纰漏的许多漏洞利用、检测方法在学术上具有一定的前沿性，在一定程度上反映了目前国内外安全技术所关注的焦点问题。

l QA工程师、软件测试人员　本书第4篇中集中介绍了产品安全性测试方面的知识，这些方法可以指导QA人员审计软件中的安全漏洞，增强软件的安全性，提高软件质量。

l 软件开发人员　知道漏洞利用原理将有利于编写出安全的代码。

l 高校信息安全专业的学生　本书将在一定程度上弥补高校教育与信息安全公司人才需求脱节的现象。用一套过硬的调试技术和逆向技术来武装自己可以让您在未来的求职道路上利于不败之地。精通exploit的人才可以轻松征服任何一家杀毒软件公司或安全资讯公司的求职门槛，获得高薪工作。

l 本科二年级以上计算机系学生　通过调试实验，你们将更加深入地了解计算机体系架构和操作系统。这些知识一样将成为您未来求职时过硬的敲门砖。

l 所有黑客技术爱好者　如果您厌倦了网络嗅探、端口扫描之类的扫盲读物，您将在本书中学到实施有效攻击所必备的知识和技巧。

关于反馈与提问

读者在阅读本书时如遇到任何问题，可以到看雪论坛相关版面参与讨论http://zeroday.pediy.com。

致谢

感谢电子工业出版社对本书的大力支持，尤其是毕宁编辑为本书出版所做的大量工作。

感谢看雪对本书的大力推荐和支持以及看雪论坛为本书提供的交流平台。

非常感谢在本书第一版问世后，向我提供勘误信息的众多热心读者，本书质量的提高离不开你们热心的帮助。

感谢赛门铁克中国响应中心的病毒分析员Beannie Cai为本书第26章友情撰稿。

最后感谢我的母校西安交通大学，是那里踏实求是的校风与校训激励着我不断进步。

Failwest

2011年5月4日