Broadview
www.broadview.com.cn

安全技术大系

看雪软件安全
http://www.pediy.com

0day安全：软件漏洞分析技术

（第2版）

王清 主编

张东辉 周浩 王继刚 赵双 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

0day安全：软件漏洞分析技术

（第2版）

王清 主编

张东辉 周浩 王继刚 赵双 编著

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

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。

图书在版编目（CIP）数据

0day 安全：软件漏洞分析技术 / 王清主编；张东辉等编著. —2 版. —北京：电子工业出版社，2011.6
（安全技术大系）
ISBN 978-7-121-13396-1

Ⅰ. ①0… Ⅱ. ①王… ②张… Ⅲ. ①计算机网络 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2011）第 074902 号

责任编辑：徐津平
印　　刷：
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　1/16　印张：48.75　字数：780 千字
印　　次：2011 年 6 月第 1 次印刷
印　　数：4000 册　　定价：85.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

关于“zero day attack”

0 day 是网络安全技术中的一个术语，特指被攻击者掌握却未被软件厂商修复的系统漏洞。

0 day 漏洞是攻击者入侵系统的终极武器，资深的黑客手里总会掌握几个功能强大的 0 day 漏洞。

0 day 漏洞是木马、病毒、间谍软件入侵系统的最有效途径。

由于没有官方发布的安全补丁，攻击者可以利用 0 day 对目标主机为所欲为，甚至在 Internet 上散布蠕虫。因此，0 day 漏洞的技术资料通常非常敏感，往往被视为商业机密。

对于软件厂商和用户来说，0 day 攻击是危害最大的一类攻击。

针对 0 day 漏洞的缓冲区溢出攻击是对技术性要求最高的攻击方式。

世界安全技术峰会 Black Hat 上每年最热门的议题之一就是“zero day attack/defense”。微软等世界著名的软件公司为了在其产品中防范“zero day attack”，投入了大量的人力、物力。

全世界有无数的信息安全科研机构在不遗余力地研究与 0 day 安全相关的课题。

全世界也有无数技术精湛的攻击者在不遗余力地挖掘软件中的 0 day 漏洞。

自　序

不请长缨，系取天骄种，剑吼西风

——《六州歌头》北宋，贺铸

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。

Failwest

再 版 序

天行健，君子以自强不息；地势坤，君子以厚德载物

——《周易》

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。

Failwest

2011 年 5 月 4 日

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’m possible”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’m possible）”的“关键（key point）”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’m possible”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，To be 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《Sword Fish（剑鱼行动）》中，Stan 在那台酷毙的计算机前坚定地说：“Nothing is 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 Native Speaker 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（Frame Work）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：

- **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。
- **信息安全理论研究者** 本书中披露的许多漏洞利用、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。
- **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。
- **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。
- **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。
- **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。
- **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。

内容导读

本书分为 5 篇，共 33 章。

第 1 篇　漏洞利用原理（初级）

第 1 章　基础知识

本章着重对漏洞挖掘中的一些基础知识进行介绍。首先是漏洞研究中的一些基本概念和原理；然后是对 Windows 平台下可执行文件的结构和内存方面的一些基础知识的介绍；最后介绍了一些漏洞分析中经常使用的软件工具。包括调试工具、反汇编工具、二进制编辑工具等。您会在后面的调试实验中反复见到这些工具的身影。在这章的最后一节，我们设计了一个非常简单的破解小实验，用于实践工具的应用，消除您对二进制的恐惧感，希望能够给您带来一些乐趣。

第 2 章　栈溢出原理与实践

基于栈的溢出是最基础的漏洞利用方法。本章首先用大量的示意图，深入浅出地讲述了操作系统中函数调用、系统栈操作等概念和原理；随后通过三个调试实验逐步讲解如何通过栈溢出，一步一步地劫持进程并植入可执行的机器代码。即使您没有任何汇编语言基础，从未进行过二进制级别的调试，在本章详细的实验指导下也能轻松完成实验，体会到 exploit 的乐趣。

第 3 章　开发 shellcode 的艺术

本章紧接第 2 章的讨论，比较系统地介绍了溢出发生后，如何布置缓冲区、如何定位 shellcode、如何编写和调试 shellcode 等实际的问题。最后两小节还给出了一些编写 shellcode 的高级技术，供有一定汇编基础的朋友作参考。

第 4 章　用 MetaSploit 开发 Exploit

MetaSploit 是软件工程中的 Frame Work（架构）在安全技术中的完美实现，它把模块化、继承性、封装等面向对象的特点在漏洞利用程序的开发中发挥得淋漓尽致。使用这个架构开发 Exploit 要比直接使用 C 语言写出的 Exploit 简单得多。本章将集中介绍如何使用这个架构进行 Exploit 开发。

第 5 章　堆溢出利用

在很长一段时间内，Windows 下的堆溢出被认为是不可利用的，然而事实并非如此。本章

将用精辟的论述点破堆溢出利用的原理，让您轻松领会堆溢出的精髓。此外，这章的一系列调试实验将加深您对概念和原理的理解。用通俗易懂的方式论述复杂的技术是本书始终坚持的原则。

第 6 章　形形色色的内存攻击技术

在了解基本的堆栈溢出后，本章将为大家展示更为高级的内存攻击技术。本章集中介绍了一些曾发表于 Black Hat 上的著名论文中所提出的高级利用技术，如狙击 Windows 异常处理机制、攻击虚函数、off by one、 Heap Spray 等利用技巧。对于安全专家，了解这些技巧和手法不至于在分析漏洞时错把可以利用的漏洞误判为低风险类型；对于黑客技术爱好者，这些知识很可能成为激发技术灵感的火花。

第 7 章　手机里的缓冲区溢出

在 PC 机上的溢出攻击进行的如火如荼的时候，您是否也想了解手机平台上的缓冲区溢出问题？那就不要错过本章！本章以 ARM 和 Windows Mobile 为例，介绍手机平台上编程和调试技巧。并在最后以一个手机上的 exploit me 为大家揭开手机里缓冲区溢出的神秘面纱。

第 8 章　其他类型的软件漏洞

缓冲区溢出漏洞只是软件漏洞的一个方面，我们来看看其他一些流行的安全漏洞。如格式化串漏洞、SQL 注入、XPath 注入、XSS 等安全漏洞产生的原因、利用技巧及防范措施。

第 2 篇　漏洞利用原理（高级）

第 9 章　Windows 安全机制概述

微软在 Windows XP SP2 和 Windows 2003 之后，向操作系统中加入了许多安全机制。本章将集中讨论这些安全机制对漏洞利用的影响。

第 10 章　栈中的守护天使：GS

针对缓冲区溢出时覆盖函数返回地址这一特征，微软在编译程序时使用了一个很酷的安全编译选项——GS。本章将对 GS 编译选项的原理进行详细介绍，并介绍几种绕过 GS 的溢出技巧。

第 11 章　亡羊补牢：SafeSEH

攻击 S.E.H 已经成为 windows 平台下漏洞利用的经典手法。为了遏制日益疯狂的攻击，微软在 Windows XP SP2 及后续版本的操作系统中引入了著名的 S.E.H 校验机制 SafeSEH。本章将会对这一安全机制进行详细的分析，并介绍其中的不足和绕过方法。

第 12 章　数据与程序的分水岭：DEP

溢出攻击的根源在于现代计算机对数据和代码没有明确区分这一先天缺陷， 而 DEP 这种

看似釜底抽薪式的防护措施是否真的可以杜绝溢出攻击呢？答案马上揭晓。

第 13 章　在内存中躲猫猫：ASLR

程序加载时不再使用固定的基址加载，ASLR 技术将溢出时使用的跳板在内存中隐藏了起来，没有了跳板我们如何溢出呢？本章将带领您在黑暗中寻找溢出的出口。

第 14 章　S.E.H 终极防护：SEHOP

SafeSEH 的败北，让微软推出一种更为严厉的 S.E.H 保护机制 SEHOP。这里将为您展示这种保护机制的犀利之处。

第 15 章　重重保护下的堆

当堆溢出变成可能后，微软不能再无视堆中的保护机制了，让我们一览堆中的保护机制，并分析其漏洞。

第 3 篇　漏洞挖掘技术

第 16 章　漏洞挖掘技术简介

不论从工程上讲还是从学术上讲，漏洞挖掘都是一个相当前沿的领域。本章将从动态测试和静态审计两方面对漏洞挖掘技术的基础知识进行简单的介绍。

第 17 章　文件类型漏洞挖掘与 Smart Fuzz

文件类型的漏洞层出不穷，持续威胁着互联网的安全。如何系统的测试文件格式，产生精确有效的畸形测试用例用以发掘文件解析器的安全漏洞，并不是一件容易的事情。本章将从理论和实践两个方面向您讲述灰盒测试技术。

第 18 章　FTP 的漏洞挖掘

本章将简述 FTP 协议，并手把手地带领您完成几个初级的漏洞测试案例，让您亲身体会下真实的漏洞长什么模样。

第 19 章　E-mail 的漏洞挖掘

E-mail 系统涉及的安全问题不光只有缓冲区溢出，在本章的挖掘案例中，您会发现除了工具和常用方法外，威力最为强大的武器还是您的大脑。Evil thinking 是安全测试中最重要的思维方式之一。

第 20 章　ActiveX 控件的漏洞挖掘

控件类漏洞曾经是大量网马的栖身之地。本章将结合若干个曾经的 0 day 向您比较系统的介绍这类漏洞的测试、调试的相关工具和方法。

第 4 篇　操作系统内核安全

第 21 章　探索 ring0

研究内核漏洞，需要首先掌握一些内核基础知识，例如内核驱动程序的开发、编译、运行和调试，内核中重要的数据结构等，本章将为读者开启探索 ring0 之门，逐步掌握一些内核基础知识。

第 22 章　内核漏洞利用技术

本章将带领读者从一个简单的内核漏洞程序 exploitme.sys 的编写开始，展示内核漏洞利用的思路、方法，以及利用程序和 Ring0 Shellcode 的编写和设计。

第 23 章　FUZZ 驱动程序

掌握了内核漏洞的原理和利用方法，本章将进入内核漏洞挖掘阶段，学习较为高级的内核漏洞挖掘技术，最后实践该漏洞挖掘技术，分析、挖掘出内核漏洞。

第 24 章　内核漏洞案例分析

本章对几种典型的内核漏洞，用几个真实的内核漏洞案例来详细分析，分析漏洞造成的具体原因和细节，并构造漏洞成功利用的方法。

第 5 篇　漏洞分析案例

第 25 章　漏洞分析技术概述

本章纵览了漏洞分析与调试的思路，并介绍了一些辅助漏洞调试分析的高级逆向工具。

第 26 章　RPC 入侵：MS06-040 与 MS08-067

由于可以做到主动式远程入侵，RPC 级别的漏洞被誉为漏洞中的王者，此类漏洞也极其稀有，每一个都有一段曲折的故事。值得一提的是最近的两个 RPC 系统漏洞竟然出自同一个函数。本章将对这个缝来补去没有修好的函数进行详细分析，让您从攻防两方面深刻理解漏洞的起因和修复策略的重要性。

第 27 章　MS06-055 分析：实战 Heap Spray

通过网页“挂马”是近年来攻击者惯用的手法。本章通过分析微软 IE 浏览器中真实的缓冲区溢出漏洞，告诉您为什么不能随便点击来历不明的 URL 链接，并在实战中为大家演示 Heap Spray 技术。

第 28 章　MS09-032 分析：一个“&”引发的血案

一个视频网页的背后可能是一只凶狠的木马，这就是著名的 Microsoft DirectShow MPEG-2

视频 ActiveX 控件远程代码执行漏洞。本章将为您分析该漏洞产生的原因及分析技巧。

第 29 章　Yahoo!Messenger 栈溢出漏洞

在波涛汹涌的溢出大潮中 Yahoo 也没能幸免，作为国外非常流行的 Yahoo!Messenger 也存在过非常严重的漏洞。本章将重现当时的场景，并分析漏洞产生的原因。

第 30 章　CVE-2009-0927：PDF 中的 JS

您可能不会随便运行一个可执行文件，但是您会想到别人发过来的 PDF 文档中也有可能隐藏着一些东西吗？本章将以 PDF 文档为例，带您领略文件类型溢出漏洞的风采。

第 31 章　坝之蚁穴：超长 URL 溢出漏洞

安全软件不一定安全，即便是这款保护未成年人健康上网的计算机终端过滤软件，也有可能成为黑客攻击的窗口。本章将介绍绿坝软件中一个已经被修复了的安全漏洞。

第 32 章　暴风影音 M3U 文件解析漏洞

晚上回家后用暴风影音打开别人发过来的 M3U 列表文件，在你陶醉于其内容之时，一只精干的小马已悄然在后台运行。想要了解这只小马是如何进入你的电脑的？请阅读本章。

第 33 章　LNK 快捷方式文件漏洞

是否我不去运行任何可疑文件，不去打开陌生的网址就安全了呢？答案是否定。LNK 快捷方式漏洞无需打开文件，只要浏览恶意文件，所在文件夹就会中毒，俗称“看一眼就挂”。本章将带您分析这一神奇的漏洞。

目　录

第 1 篇　漏洞利用原理（初级）