第一图书网, tushu007.com

<<0day安全 （第2版）>>

图书基本信息

书名：<<0day安全 （第2版）>>

13位ISBN编号：9787121133961

10位ISBN编号：7121133962

出版时间：2011-6

出版时间：电子工业出版社

作者：王清 主编

页数：753

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

内容概要

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。

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做参考。

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。

作者简介

王清　网络ID：Failwest。
著名信息安全专家，于2008年出版《Odav安全：软件漏洞分析技术》一书。
拥有多年的安全审计、安全测试经验。
熟悉各类软件安全问题，擅长二进制级别的漏洞调试与分析，Web应用的安全审计以及无线电协议的安全审计等。

书籍目录

第1篇 漏洞利用原理（初级）
第1章 基础知识
1.1 漏洞概述
1.1.1 bug与漏洞
1.1.2 几个令人困惑的安全问题
1.1.3 漏洞挖掘、漏洞分析、漏洞利用
1.1.4 漏洞的公布与0 day响应
1.2 二进制文件概述
1.2.1 PE文件格式
1.2.2 虚拟内存
1.2.3 PE文件与虚拟内存之间的映射
1.3 必备工具
1.3.1 OllyDbg简介
1.3.2 SoftICE简介
1.3.3 WinDbg简介
1.3.4 IDA Pro简介
1.3.5 二进制编辑器
1.3.6 VMware简介
1.3.7 Python编程环境
1.4 Crack小实验
第2章 栈溢出原理与实践
2.1 系统栈的工作原理
2.1.1 内存的不同用途
2.1.2 栈与系统栈
2.1.3 函数调用时发生了什么
2.1.4 寄存器与函数栈帧
2.1.5 函数调用约定与相关指令
2.2 修改邻接变量
2.2.1 修改邻接变量的原理
2.2.2 突破密码验证程序
2.3 修改函数返回地址
2.3.1 返回地址与程序流程
2.3.2 控制程序的执行流程
2.4 代码植入
2.4.1 代码植入的原理
2.4.2 向进程中植入代码
第3章 开发shellcode的艺术
3.1 shellcode概述
3.1.1 shellcode与exploit
3.1.2 shellcode需要解决的问题
3.2 定位shellcode
3.2.1 栈帧移位与jmp esp
3.2.2 获取“跳板”的地址
3.2.3 使用“跳板”定位的exploit
3.3 缓冲区的组织

3.3.1 缓冲区的组成
3.3.2 抬高栈顶保护shellcode
3.3.3 使用其他跳转指令
3.3.4 不使用跳转指令
3.3.5 函数返回地址移位
3.4 开发通用的shellcode
3.4.1 定位API的原理
3.4.2 shellcode的加载与调试
3.4.3 动态定位API地址的shellcode
3.5 shellcode编码技术
3.5.1 为什么要对shellcode编码
3.5.2 会“ 变形 ”的shellcode
3.6 为shellcode“ 减肥 ”
3.6.1 shellcode瘦身大法
3.6.2 选择恰当的hash算法
3.6.3 191个字节的bindshell
第4章 用MetaSploit开发Exploit
4.1 漏洞测试平台MSF 简介
4.2 入侵Windows系统
4.2.1 漏洞简介
4.2.2 图形界面的漏洞测试
4.2.3 console界面的漏洞测试
4.3 利用MSF制作shellcode
4.4 用MSF扫描“ 跳板 ”
4.5 Ruby语言简介
4.6“ 傻瓜式 ”Exploit开发
4.7 用MSF发布POC
第5章 堆溢出利用
5.1 堆的工作原理
5.1.1 Windows堆的历史
5.1.2 堆与栈的区别
5.1.3 堆的数据结构与管理策略
5.2 在堆中漫游
5.2.1 堆分配函数之间的调用关系
5.2.2 堆的调试方法
5.2.3 识别堆表
5.2.4 堆块的分配
5.2.5 堆块的释放
5.2.6 堆块的合并
5.2.7 快表的使用
5.3 堆溢出利用（上）——DWORD SHOOT
5.3.1 链表“ 拆卸 ”中的问题
5.3.2 在调试中体会“ DWORD SHOOT ”
5.4 堆溢出利用（下）——代码植入
5.4.1 DWORD SHOOT的利用方法
5.4.2 狙击P.E.B中RtlEnterCritical-Section()的函数指针
5.4.3 堆溢出利用的注意事项

第6章 形形色色的内存攻击技术
6.1 狙击Windows异常处理机制
6.1.1 S.E.H概述
6.1.2 在栈溢出中利用S.E.H
6.1.3 在堆溢出中利用S.E.H
6.1.4 深入挖掘Windows异常处理
6.1.5 其他异常处理机制的利用思路
6.2 “ off by one ”的利用
6.3 攻击C++的虚函数
6.4 Heap Spray：堆与栈的协同攻击
第7章 手机里的缓冲区溢出
7.1 Windows Mobile简介
7.1.1 Windows Mobile前世今生
7.1.2 Windows Mobile架构概述
7.1.3 Windows Mobile的内存管理
7.2 ARM简介
7.2.1 ARM是什么
7.2.2 ARM寄存器结构
7.2.3 ARM汇编指令结构
7.2.4 ARM指令寻址方式
7.2.5 ARM的函数调用与返回
7.3 Windows Mobile上的HelloWorld
7.4 远程调试工具简介
7.4.1 远程信息查看管理套件
7.4.2 手机上的调试——Microsoft Visual Studio
7.4.3 手机上的调试——IDA
7.5 手机上的exploit me
第8章 其他类型的软件漏洞
8.1 格式化串漏洞
8.1.1 printf中的缺陷
8.1.2 用printf读取内存数据
8.1.3 用printf向内存写数据
8.1.4 格式化串漏洞的检测与防范
8.2 SQL注入攻击
8.2.1 SQL注入原理
8.2.2 攻击PHP+MySQL网站
8.2.3 攻击ASP+SQL Server网站
8.2.4 注入攻击的检测与防范
8.3 其他注入方式
8.3.1 Cookie注入，绕过马其诺防线
8.3.2 XPath注入，XML的阿喀琉斯之踵
8.4 XSS攻击
8.4.1 脚本能够“ 跨站 ”的原因
8.4.2 XSS Reflection攻击场景
8.4.3 Stored XSS攻击场景
8.4.4 攻击案例回顾：XSS蠕虫
8.4.5 XSS的检测与防范

8.5 路径回溯漏洞
8.5.1 路径回溯的基本原理
8.5.2 范式化与路径回溯
第2篇 漏洞利用原理（高级）
第9章 Windows安全机制概述
第10章 栈中的守护天使：GS
10.1 GS安全编译选项的保护原理
10.2 利用未被保护的内存突破GS
10.3 覆盖虚函数突破GS
10.4 攻击异常处理突破GS
10.5 同时替换栈中和.data中的Cookie突破GS
第11章 亡羊补牢：SafeSEH
11.1 SafeSEH对异常处理的保护原理
11.2 攻击返回地址绕过SafeSEH
11.3 利用虚函数绕过SafeSEH
11.4 从堆中绕过SafeSEH
11.5 利用未启用SafeSEH模块绕过SafeSEH
11.6 利用加载模块之外的地址绕过SafeSEH
11.7 利用Adobe Flash Player ActiveX控件绕过SafeSEH
第12章 数据与程序的分水岭：DEP
12.1 DEP机制的保护原理
12.2 攻击未启用DEP的程序
12.3 利用Ret2Libc挑战DEP
12.3.1 Ret2Libc实战之利用ZwSetInformationProcess
12.3.2 Ret2Libc实战之利用VirtualProtect
12.3.3 Ret2Libc实战之利用VirtualAlloc
12.4 利用可执行内存挑战DEP
12.5 利用.NET挑战DEP
12.6 利用Java applet挑战DEP
第13章 在内存中躲猫猫：ASLR
13.1 内存随机化保护机制的原理
13.2 攻击未启用ASLR的模块
13.3 利用部分覆盖进行定位内存地址
13.4 利用Heap spray技术定位内存地址
13.5 利用Java applet heap spray技术定位内存地址
13.6 为.NET控件禁用ASLR
第14章 S.E.H终极防护：SEHOP
14.1 SEHOP的原理
14.2 攻击返回地址
14.3 攻击虚函数
14.4 利用未启用SEHOP的模块
14.5 伪造S.E.H链表
第15章 重重保护下的堆
15.1 堆保护机制的原理
15.2 攻击堆中存储的变量
15.3 利用chunk重设大小攻击堆
15.4 利用Lookaside表进行堆溢出

第3篇 漏洞挖掘技术
第16章 漏洞挖掘技术简介
16.1 漏洞挖掘概述
16.2 动态测试技术
16.2.1 SPIKE简介
16.2.2 beSTORM简介
16.3 静态代码审计
第17章 文件类型漏洞挖掘 与Smart Fuzz
17.1 Smart Fuzz概述
17.1.1 文件格式Fuzz的基本方法
17.1.2 Blind Fuzz和Smart Fuzz
17.2 用Peach挖掘文件漏洞
17.2.1 Peach介绍及安装
17.2.2 XML介绍
17.2.3 定义简单的 Peach Pit
17.2.4 定义数据之间的依存关系
17.2.5 用Peach Fuzz PNG文件
17.3 010脚本，复杂文件解析的瑞士军刀
17.3.1 010 Editor简介
17.3.2 010脚本编写入门
17.3.3 010脚本编写提高——PNG文件解析
17.3.4 深入解析，深入挖掘——PPT文件解析
第18章 FTP的漏洞挖掘
18.1 FTP协议简介
18.2 漏洞挖掘手记1：DOS
18.3 漏洞挖掘手记2：访问权限
18.4 漏洞挖掘手记3：缓冲区溢出
18.5 漏洞挖掘手记4：Fuzz DIY
第19章 E-Mail的漏洞挖掘
19.1 挖掘SMTP漏洞
19.1.1 SMTP协议简介
19.1.2 SMTP漏洞挖掘手记
19.2 挖掘POP3漏洞
19.2.1 POP3协议简介
19.2.2 POP3漏洞挖掘手记
19.3 挖掘IMAP4漏洞
19.3.1 IMAP4协议简介
19.3.2 IMAP4漏洞挖掘手记
19.4 其他E-mail漏洞
19.4.1 URL中的路径回溯
19.4.2 内存中的路径回溯
19.4.3 邮件中的XSS
第20章 ActiveX控件的漏洞挖掘
20.1 ActiveX控件简介
20.1.1 浏览器与ActiveX控件的关系
20.1.2 控件的属性
20.2 手工测试ActiveX控件

20.2.1 建立测试模板
20.2.2 获取控件的接口信息
20.3 用工具测试ActiveX控件：COMRaider
20.4 挖掘ActiveX漏洞
20.4.1 ActiveX漏洞的分类
20.4.2 漏洞挖掘手记1：超星阅读器溢出
20.4.3 漏洞挖掘手记2：目录操作权限
20.4.4 漏洞挖掘手记3：文件读权限
20.4.5 漏洞挖掘手记3：文件删除权限
第4篇 操作系统内核安全
第21章 探索ring0
21.1 内核基础知识介绍
21.1.1 内核概述
21.1.2 驱动编写之Hello World
21.1.3 派遣例程与IRP结构
21.1.4 Ring3打开驱动设备
21.1.5 DeviceIoControl函数与IoControlCode
21.1.6 Ring3/Ring0的四种通信方式
21.2 内核调试入门
21.2.1 创建内核调试环境
21.2.2 蓝屏分析
21.3 内核漏洞概述
21.3.1 内核漏洞的分类
21.3.2 内核漏洞的研究过程
21.4 编写安全的驱动程序
21.4.1 输入输出检查
21.4.2 验证驱动的调用者
21.4.3 白名单机制的挑战
第22章 内核漏洞利用技术
22.1 利用实验之exploitme.sys
22.2 内核漏洞利用思路
22.3 内核漏洞利用方法
22.4 内核漏洞利用实战与编程
22.5 Ring0 Shellcode的编写
第23章 FUZZ驱动程序
23.1 内核FUZZ思路
23.2 内核FUZZ工具介绍
23.3 内核FUZZ工具DIY
23.3.1 Fuzz对象、Fuzz策略、Fuzz项
23.3.2 IoControl MITM Fuzz
23.3.3 IoControl Driver Fuzz
23.3.4 MyIoControl Fuzzer界面
23.4 内核漏洞挖掘实战
23.4.1 超级巡警ASTDriver.sys本地提权漏洞
23.4.2 东方微点mp110013.sys本地提权漏洞
23.4.3 瑞星HookCont.sys驱动本地拒绝服务漏洞
第24章 内核漏洞案例分析

24.1 远程拒绝服务内核漏洞
24.2 本地拒绝服务内核漏洞
24.3 缓冲区溢出内核漏洞
24.4 任意地址写任意数据内核漏洞
24.5 任意地址写固定数据内核漏洞
第5篇 漏洞分析案例
第25章 漏洞分析技术概述
25.1 漏洞分析的方法
25.2运动中寻求突破：调试技术
25.2.1 断点技巧
25.2.2 回溯思路
25.3 用“白眉”在PE中漫步
25.3.1 指令追踪技术与Paimei
25.3.2 Paimei的安装
25.3.3 使用PE Stalker
25.3.4 迅速定位特定功能对应的代码
25.4 补丁比较
第26章 RPC入侵：MS06-040 与MS08-067
26.1 RPC漏洞
26.1.1 RPC漏洞简介
26.1.2 RPC编程简介
26.2 MS06-040
26.2.1 MS06-040简介
26.2.2 动态调试
26.2.3 静态分析
26.2.4 实现远程exploit
26.3 Windows XP环境下的MS06-040 exploit
26.3.1 静态分析
26.3.2 蠕虫样本的exploit方法
26.3.3 实践跨平台exploit
26.4 MS08-067
26.4.1 MS08-067简介
26.4.2 认识Legacy Folder
26.4.3“移经”测试
26.4.4“移经”风险
26.4.5 POC的构造
26.5 魔波、Conficker与蠕虫病毒
第27章 MS06-055分析：实战Heap Spray
27.1 MS06-055简介
27.1.1 矢量标记语言（VML）简介
27.1.2 0 day安全响应纪实
27.2 漏洞分析
27.3 漏洞利用
第28章 MS09-032分析：一个“&”引发的血案
28.1 MS09-032简介
28.2 漏洞原理及利用分析
第29章 Yahoo!Messenger栈 溢出漏洞

29.1 漏洞介绍
29.2 漏洞分析
29.3 漏洞利用
第30章 CVE-2009-0927：PDF中的JS
30.1 CVE-2009-0927简介
30.2 PDF文档格式简介
30.3 漏洞原理及利用分析
第31章 坝之蚁穴：超长URL溢出漏洞
31.1 漏洞简介
31.3 漏洞原理及利用分析
第32章 暴风影音M3U文件解析漏洞
32.1 漏洞简介
32.2 M3U文件简介
32.3 漏洞原理及利用分析
第33章 LNK快捷方式文件漏洞
33.1 漏洞简介
33.2 漏洞原理及利用分析
附录A 已公布的内核程序漏洞列表
参考文献

编辑推荐

王清主编的《Oday安全：软件漏洞分析技术（第2版）》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。
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。

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com