<<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

<<0day安全 （第2版）>>

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。

<<0day安全 （第2版）>>

书籍目录

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。

版权说明