<<0day安全：软件漏洞分析技>>

图书基本信息

书名：<<0day安全：软件漏洞分析技术>>

13位ISBN编号：9787121060779

10位ISBN编号：7121060779

出版时间：2008

出版时间：电子工业出版社

作者：王清

页数：358

前言

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。

<<0day安全：软件漏洞分析技>>

内容概要

分为4篇17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。第一篇为常用工具和基础知识的介绍；第二篇从攻击者的视角出发，揭秘了攻击者利用漏洞的常用伎俩，了解这些知识对进行计算机应急响应和提高软件产品安全性至关重要；第三篇在第二篇的基础上，从安全专家的角度介绍了漏洞分析和计算机应急响应方面的知识；第四篇则站在软件工程师的角度讲述如何在开发、测试等软件生命周期的各个环节中加入安全因素，以增强软件产品的安全性。

作者简介

王清，网络ID：failwest，于西安交通大学先后获得计算机科学与技术学士学位、系统工程专业硕士学位。
曾工作于教育部下一代互联网与网络安全重点实验室，研究兴趣涉及蠕虫建模、高级IDS算法、网站安全、代码审计、漏洞分析、病毒分析、逆向工程等领域。
现就职于Symantec产品安全部，从事软件攻击测试，系统安全性审计，安全咨询等工作。

<<0day安全：软件漏洞分析技>>

书籍目录

章节摘录

第6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。
第6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7章　Windows异常处理机制深入浅出对异常处理的利用是Windows平台下缓冲区溢出漏洞利用的一大特点。
第7章除了介绍如何在溢出发生时利用S.E.H外，还对Windows异常处理机制做了较深入的剖析，供有一定基础的读者参考。
第8章　高级内存攻击技术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。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。

后记

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。
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。

编辑推荐

《oday安全：软件漏洞分析技术》为我们系统介绍了漏洞分析的原理和技术细节，并深入浅出地引用了不少在安全界非常经典的漏洞实例。
然而，更重要的是failwest并没有流水账式的罗列知识与技术，而是花了大量的篇幅介绍了漏洞检测的步骤及其背后的思维方式。
这些完全不同的思维方式，加上分析员必备的技能以及必需的工具，为读者展现了一套非常完整的软件漏洞分析方法。

名人推荐

从软件开发者的角度著书阐述漏洞分析与检测技术的专业软件工程师。
作者非常恰当地把着眼点放在一个软件开发者的角度去做漏洞检测，使得《0 day安全：软件漏洞分析技术》对大多数读者来说更加实用。
《0 day安全：软件漏洞分析技术》为我们系统介绍了漏洞分析的原理和技术细节，并深入浅出地引用了不少在安全界非常经典的漏洞实例。
然而，更重要的是failwest并没有流水账式的罗列知识与技术，而是花了大量的篇幅介绍了漏洞检测的步骤及其背后的思维方式。
这些完全不同的思维方式，加上分析员必备的技能以及必需的工具，为读者展现了一套非常完整的软件漏洞分析方法。
许　明

版权说明