<<暗战亮剑>>

图书基本信息

书名：<<暗战亮剑>>

13位ISBN编号：9787115228703

10位ISBN编号：7115228701

出版时间：2010-7

出版时间：人民邮电出版社

作者：王继刚，曲慧文，王刚　编著

页数：300

字数：459000

前言

还记得2002年，当我第一次依靠自己所学的知识，独立发现了Windows2000系统下存在的一个缓冲区溢出漏洞的时候，我激动地从宿舍里冲出来拥抱每一位我并不认识的同学。
长久以来，国内对于软件安全漏洞的研究还处在起步阶段，能够参考的资料也都是满篇英文的外国文献。
看一看国内外的很多安全资料、安全图书，大多都是讲解分析软件安全漏洞的原理。
作为一名软件安全的研究人员，即使能够将所有的软件漏洞原理都滚瓜烂熟地背出来，也无法发现一个软件安全漏洞，因为只知道“果”而不知道“因”，完全处于一个光知道理论，却不知道如何入手发现软件安全漏洞的朦胧状态。
我们需要实践，更需要依靠自己的能力去发现软件安全漏洞，这是一切研究的前提。
而惟一能够解决这个困境的方法，就是出版一本真正讲解如何发现软件安全漏洞全过程的图书，提供读者参考，带领读者全面了解一个软件安全漏洞从发掘到被利用的前因后果，这样才能够将软件安全变成一门能够让读者学得会、用得上的技术。
很长时间以来，我一直在国内一本著名的安全杂志上发表安全技术文章，这些文章全都是我自己独立发现软件安全漏洞的实践。
很多读者通过各种渠道询问我：究竟是如何发现这些安全漏洞的，又怎么知道某软件存在安全漏洞等。
读者的热情使我觉得有必要将自己知道的东西写出来，因为，一旦掌握了如何发现软件安全漏洞，读者的安全技术水平定会得到很大的提高。
为了能够将软件漏洞发掘技术写得通俗明了，让每一位读者都能够看懂学懂，我对本书进行了多次的修改，挑选出软件漏洞发掘技术中最为通用的部分进行讲解，目的就是希望每一位阅读本书的读者，能够用书中学到的知识发现第一个属于自己的软件安全漏洞，那不仅属于你的成功，也是对我最大的肯定。
在创作本书的过程中，我特别注重讲解动手实践的过程。
为此，本书在整体结构上更加突出了让读者自己动手实践的内容。
本书以实践课的形式，将每一种软件安全漏洞的具体发现过程以图文并茂的方式呈现给读者，以案例为线索，详细讲解软件安全漏洞攻防技术与实战技巧。
加之为本书配套的视频教程，更方便读者理解软件漏洞发掘技术的具体细节，几乎做到了“一看就会”。
同时，为了能够让读者理解软件安全漏洞的危害，还对每种安全漏洞的利用方法进行了解析，最后又补充上每种安全漏洞的具体防范方法，做到了攻防兼备。
本书有3个非常重要的特点。
一是首度揭示了对安全防护软件漏洞的发掘技术。
我们平时为了防范黑客的恶意攻击，都会在自己的计算机系统上安装杀毒软件或者防火墙软件，殊不知这些本身用来保护计算机系统安全的软件，可能也存在着可怕的安全漏洞。
由于种种原因，针对安全防护软件漏洞发掘技术的资料很少，在这里我将与读者一起分享。
二是写出了如何发掘系统内核中存在的安全漏洞。
一直以来，系统内核都是一个禁区，这是因为系统内核的权限不同于普通软件，它拥有计算机软件层面最高的权限，一旦它中间出现了安全漏洞，那么整个软件安全体系就形同虚设了。
本书以多个真实的案例，讲解了系统内核中安全漏洞发生的原因与发现的方法，是关注内核安全读者的一个很好的学习机会。
三是随书附送的光盘中，为读者提供了《黑客防线》的“爱无言”老师所制作的软件漏洞发掘视频教程，这是一个极具学习和参考价值的视频资料。
同时，本书作者也结合书中的内容特意制作了一套详细的教学视频，通过这些视频资料，读者可以更好地学习到软件安全漏洞发掘技术的精髓，可以按照视频教程的指导边操作边学习，在最大程度上深入理解本书的内容。

<<暗战亮剑>>

内容概要

本书采用通俗易懂的语言，将软件漏洞的发掘过程清晰地展现给每一位读者。
全书分为10章。
第1章介绍常见的软件漏洞，及这些漏洞出现的原因和危害；第2章主要讲解建立发掘软件安全漏洞的环境；第3章～第9章全面讲解针对不同类型软件的安全漏洞应该采取的漏洞发掘方法。
同时结合实际操作和案例解析的方式带领读者学习；第10章针对普通的软件用户和专业的软件开发者，分别给出了如何防范针对软件漏洞的恶意攻击和预防软件出现漏洞的方法。
　　本书实践性强，第一次以具体软件漏洞案例的形式向读者揭示了软件漏洞是怎样被发现，又怎样被利用的全过程。
在讲述软件漏洞发掘技术的时候，将软件漏洞的危害性、破坏性一起告诉读者，目的是为了让读者在明白如何发现漏洞的时候，更知道如何防范软件漏洞。
随书附送的光盘中，为读者提供了软件漏洞发掘的视频教程，这是一个极具学习和参考价值的视频教程。
　　本书不仅从软件安全研究人员的角度谈论如何发现软件漏洞，也从软件开发者的角度给出了防止软件出现漏洞的方法，以帮助软件编程人员开发出安全的软件系统。
　　本书适合所有关注软件安全的人们，尤其是从事软件安全测试的读者。
同时，本书也可以作为计算机安全培训及高等院校的教材和参考书。

<<暗战亮剑>>

作者简介

王继刚，笔名“爱无言”，现任某安全部门技术总监，长期在国内著名黑客杂志《黑客防线》、《黑客手册》、《黑客×档案》上发表安全漏洞分析文章，独立发现过多个操作系统、应用软件、网络程序的漏洞。
现在为《黑客防线》特约作者。
同时，是国内著名黑客组织“邪恶八进制”核心成员，主要擅长于逆向分析技术与软件安全测试。
曲慧文，自由安全研究者，是国内为数不多的“女黑客”之一，黑客类杂志长期撰稿人，多个著名安全漏洞的发现者，在服务器渗透和Web应用程序漏洞发掘方面有着独到的见解。

<<暗战亮剑>>

书籍目录

第1章　无法摆脱的漏洞　1.1　软件漏洞的概念　1.2　软件漏洞的分类　1.2.1　缓冲区溢出漏洞　1.2.2　整数溢出漏洞　1.2.3　格式化字符串漏洞　1.2.4　指针覆盖漏洞　1.2.5　SQL注入漏洞　1.2.6　Bypass漏洞　1.2.7　信息泄露漏洞　1.2.8　越权型漏洞　1.3　软件漏洞的危害　1.3.1　无法正常使用　1.3.2　引发恶性事件　1.3.3　关键数据丢失　1.3.4　秘密信息泄露　1.3.5　被安装木马病毒　1.4　安全漏洞出现的原因　1.4.1　小作坊式的软件开发　1.4.2　赶进度带来的弊端　1.4.3　被轻视的软件安全测试　1.4.4　淡薄的安全思想　1.4.5　不完善的安全维护　1.5　做一名软件安全的维护者　第2章　建立软件漏洞发掘环境　2.1　虚拟机的安装　2.1.1　虚拟机的概念　2.1.2　为什么选择虚拟机　2.1.3　VMware的基本使用　2.2　IIS的安装　2.3　用XAMPP建立网站环境　2.4　软件漏洞发掘的基本步骤　2.4.1　提供源代码的情况　2.4.2　没有源代码的情况　2.5　软件漏洞发掘中需要注意的问题　2.5.1　漏洞成因的确定　2.5.2　漏洞危害的确定　2.5.3　多平台下的测试　第3章　文字处理型软件的漏洞剖析　3.1　何谓文字处理型软件　3.2　文字处理型软件漏洞的发掘思想　3.2.1　主动的功能测试　3.2.2　被动的输入性测试　3.2.3　两个漏洞发掘工作必备的软件　3.3　发掘文字处理型软件漏洞的难点　3.3.1　文件格式的不公开　3.3.2　手工测试任务量大　3.4　发掘漏洞软件FileFuzz的出现　3.5　实战课之一：使用FileFuzz发掘文字处理软件漏洞　3.6　文字处理型软件漏洞的危害与利用　3.6.1　ShellCode与木马植入　3.6.2　本地权限与系统命令　3.6.3　邮件附件中的隐蔽杀手　3.7　实战课之二：编写属于自己的发掘漏洞程序　3.8　媒体播放软件的漏洞发掘　3.9　文件处理型软件的漏洞发掘　3.10　FileFuzz程序的弊端　3.10.1　不善于发掘明文式漏洞　3.10.2　时间消耗大　3.10.3　误报几率高　3.10.4　盲目性大　3.11　FileFuzz程序的发展方向　3.11.1　自动判断文件格式　3.11.2　框架式的组成　3.11.3　自动分析与回溯测试　3.12　防范漏洞攻击的方法　3.12.1　及时升级软件补丁　3.12.2　防范来路不明的文档　3.13　小结　第4章　实战远程服务型软件的漏洞发掘　第5章　浏览器软件的漏洞发掘第6章　实战ActiveX控件的安全漏洞发掘　第7章　实战开源软件的安全漏洞发掘　第8章　安全防护软件漏洞攻防　第9章　系统内核里发掘漏洞　第10章　全面防范软件漏洞　附录A　一个发送自定义TCP数据包的Visual C++程序　附录B　一个驱动程序的完整实现程序　参考文献

章节摘录

插图：不知道此刻正在看这本书的你是不是有过这样的经历：新买的计算机刚刚连上因特网才几天的时间，就发现计算机开始变得运行缓慢、反应迟钝。
使用杀毒软件查杀计算机，试图能够发现隐藏在计算机中的木马病毒程序，可是，最后的结果是连杀毒软件竟然都无法正常打开，遂怀疑自己的计算机被人攻击了，于是重新给计算机安装上新的操作系统，接着安装最新的杀毒软件、防火墙软件，心想这下子不会再中毒了，于是放心大胆地开始上网，几天后再次发现计算机又中毒了！
这种经历相信很多读者都曾有过或者见到过，其实在你判断到自己的计算机中毒的时候，你的思路还是正确的，然而当再次中毒的时候，你就应该发现这里的问题不再是那么简单，无论是最新的杀毒软件，还是防火墙软件都无法阻止中毒，那么这些令人发狂的木马病毒程序又是从哪里进入计算机的呢？
此刻，我们终于进入了主题，因为这本书讨论的内容也许正好就解释了前面那道困扰了很多人的难题。
对于一般的计算机使用者来说，认为给计算机安装上最新的杀毒软件，安装上最新的防火墙软件，就可以防止自己的计算机被木马病毒感染，甚至可以阻止无所不能的“黑客”攻击。
如果计算机安全可以用这样简单的方法就全面保护，那么怎么还能听说某某国家的政府计算机全部被恶意攻击造成瘫痪，损失惨重呢。
这说明，计算机安全要比我们想象的复杂和深奥得多，而这里面最重要的一个问题就是本书将要介绍的——软件安全漏洞。
软件的定义范围是很广的，我们使用的计算机其实就是计算机的俗称，一台计算机是由硬件以及软件两个部分组成，单纯地在计算机市场买到的就是计算机的硬件，我们要想使用这些硬件，就必须安装软件，而这里最基本的软件就是操作系统。
软件一旦在计算机系统里运行起来，就称之为“程序”。
但是，计算机软件是由人编写开发出来的，准确地说是计算机程序员开发出来的，既然是这样，每一个计算机程序员的编程水平不一样，就会造成软件存在这样或者那样的问题。
这些问题可能隐藏得很深，在使用软件的过程中不会轻易体现出来。

媒体关注与评论

本书比较全面地讨论了各类软件安全漏洞的测试方法。
作者通过丰富的案例，生动、深入地向读者讲述了软件安全性测试(penetration testing)的核心思想，非常适合热爱软件安全的读者学习。
——《Oday安全：软件漏洞分析技术》作者failwest(王清)

<<暗战亮剑>>

编辑推荐

《暗战亮剑:软件漏洞发掘与安全防范实战》：19个综合案例演示，全面分析漏洞的成因与发掘方法利用Fuzzing技术，陕速发掘出软件中潜在的安全漏洞利用旧P探测系统内核Ring0层中的重大安全隐患使用代码审计技术找出源程序中的Bug指导读者编程实现刚eFuzz程序230分钟的视频指导读者全面学习和理解书中内容

版权说明