高等院校信息安全专业系列教材

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

Foundation of Exploitation and Penetration Testing

漏洞利用及渗透测试基础

刘哲理 李进 贾春福 编著

Information Security

http://www.tup.com.cn

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

高等院校信息安全专业系列教材

Foundation of Exploitation and Penetration Testing

漏洞利用及渗透测试基础

刘哲理 李进 贾春福 编著

http://www.tu

Information Security

清华大学出版社
北京

内 容 简 介

本书主要包含三部分内容：第一部分介绍信息安全的基础知识，包括堆栈基础、汇编语言、PE 文件格式、信息安全专业必知必会的基础工具 OllyDBG 和 IDA Pro 等；第二部分通过部分简单案例深入浅出地介绍漏洞利用及漏洞挖掘的原理，旨在让读者能直观地认识漏洞的危害性，了解漏洞挖掘的基本思想和流程；第三部分则针对渗透测试及 Web 应用安全进行详细讲解，包括渗透测试框架 Metasploit、针对 Window XP 系统的扫描和渗透、Web 应用开发原理、Web 应用的安全威胁、针对 Web 的渗透攻击等，其中基于 Web 的渗透测试对很多读者而言很容易上手实践，通过跟随本书的案例可以加深对黑客攻防的认识。

本书是南开大学信息安全专业的必修课教材，建议在大二下学期使用。对于信息安全专业的学生而言，这是一本较为基础、全面的入门级教程；对于非信息安全专业的学生，如果想了解一些软件安全、Web 安全的知识，甚至仅仅是想知道黑客是怎么炼成的，也非常值得推荐来读一读。

图书在版编目(CIP)数据

漏洞利用及渗透测试基础/刘哲理，李进，贾春福编著. —北京：清华大学出版社，2017
(高等院校信息安全专业系列教材)
ISBN 978-7-302-46418-1

Ⅰ. ①漏… Ⅱ. ①刘… ②李… ③贾… Ⅲ. ①计算机网络－安全技术－高等学校－教材
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 023659 号

责任编辑：梁　颖
封面设计：何凤霞
责任校对：白　蕾
责任印制：沈　露

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795954

印 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：13　　**字　数**：298 千字
版　　次：2017 年 3 月第 1 版　　**印　次**：2017 年 3 月第1 次印刷
印　　数：1～1500
定　　价：39.50 元

产品编号：072905-01

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专

家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时5年，制定出我国第一个信息安全专业指导性专业规范，于2012年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》（由清华大学出版社正式出版）。“高等院校信息安全专业系列教材”在教育部高等学校信息安全专业教学指导委员会的指导下，根据《高等学校信息安全专业指导性专业规范》组织编写和修订，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断完善。

我们的E-mail地址：zhangm@tup.tsinghua.edu.cn；联系人：张民。

“高等院校信息安全专业系列教材”编审委员会

前言

当今我们已经处在互联网时代，黑客入侵、隐私数据泄露、网络诈骗等各类安全事件频发之中，人们只知道所处的网络不安全、使用的软件有危险、黑客容易入侵，但是却不知道这些安全事件发生的真正原因。

写这本书的目的就源于此。一方面，期望为信息安全专业的学生提供全面、概括的入门级教程，培养其信息安全攻防的兴趣；另一方面，希望为那些对信息安全、黑客攻防感兴趣的计算机或软件专业的学生，融合软件安全、Web 安全和黑客攻防多维知识，提供一些概况性解答。

如果想知道系统为什么不安全、黑客轻松就可以入侵的原因，只需要通过本书读懂漏洞的概念、知道漏洞的危害性即可。如果想知道黑客如何进行攻击，可以通过本书读懂渗透测试，动手实践针对 Web 网站的 SQL 注入等攻击。如果想知道漏洞产生的根本原因，并且渴望知道如何让这个网络时代的系统、软件、网站更加安全，那么恭喜你，你已经了解了本书编写的初衷和精髓，那就是如何编写安全的代码。代码审计、必要的渗透测试，才会确保发布的软件系统、编写的网站程序漏洞尽可能减少，让互联网时代里黑客可利用的资源尽可能耗尽。

本教材由刘哲理（南开大学）、李进（广州大学）共同编写完成，由贾春福（南开大学）教授对知识点和内容进行了摘选和校正。在编写过程中采用编者长期使用的讲稿，并参考了相关书籍和网络资料，在此对相关作者表示诚挚的谢意。由于编者水平有限，书中难免存在疏漏，敬请同行专家批评指正。

刘哲理

2016-10-01

目 录

第1章 绪 论

学习要求：掌握病毒、蠕虫和木马的概念与区别；了解漏洞产业链，认识漏洞产生的主要原因；掌握渗透测试的概念，了解渗透测试的分类。

课时：2课时。

1.1 病毒和木马

在信息化时代，人们发现在维持公开的 Internet 连接的同时保护网络和计算机系统的安全变得越来越困难。病毒、木马、后门、蠕虫攻击层出不穷，虚假网站的钓鱼行为也让警惕性不高的公众深受其害。大家都深知病毒、木马、后门和蠕虫的危险，并深恶痛绝，但是对它们又知之甚少，甚至区分不开什么是病毒，什么是木马。

病毒、木马和蠕虫是可导致计算机和计算机上的信息损坏的恶意程序。它们可能使网络和操作系统变慢，危害严重时甚至会完全破坏整个系统，并且还可能基于所驻主机向周围传播，在更大范围内造成危害。这三种东西都是人为编制出的恶意代码，都会对用户造成危害，人们往往将它们统称为病毒，但其实这种称法并不准确，它们之间虽然有着共性，但也有着很大的差别。

1.1.1 病毒

计算机病毒(Computer Virus)，根据《中华人民共和国计算机信息系统安全保护条例》，病毒的明确定义是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

病毒必须满足两个条件：

(1) 它必须能自行执行。它通常将自己的代码置于另一个程序的执行路径中。

(2) 它必须能自我复制。例如，它可能用受病毒感染的文件副本替换其他可执行文件。病毒既可以感染桌面计算机也可以感染网络服务器。

此外，病毒往往还具有很强的感染性、一定的潜伏性、特定的触发性和很大的破坏性等，由于计算机所具有的这些特点与生物学上的病毒有相似之处，因此人们才将这种恶意程序代码称之为“计算机病毒”。一些病毒被设计为通过损坏程序、删除文件或重新格式化硬盘来损坏计算机。有些病毒不损坏计算机，而只是复制自身，并通过显示文本、视频和音频消息表明它们的存在。即使是这些良性病毒也会给计算机用户带来问题。通常它

们会占据合法程序使用的计算机内存，结果会引起操作异常，甚至导致系统崩溃。另外，许多病毒包含大量错误，这些错误可能导致系统崩溃和数据丢失。

1.1.2 蠕虫

蠕虫(Worm)病毒是一种常见的计算机病毒，它利用网络进行复制和传播，传染途径是通过网络和电子邮件。最初的蠕虫病毒定义是因为在DOS环境下，病毒发作时会在屏幕上出现一条类似虫子的东西，胡乱吞吃屏幕上的字母并将其改形。蠕虫病毒是自包含的程序(或是一套程序)，它能传播自身功能的拷贝或自身的某些部分到其他的计算机系统中(通常是经过网络连接)。

蠕虫是一种通过网络传播的恶性病毒，它具有病毒的一些共性，如传播性、隐蔽性、破坏性等，同时具有自己的一些特征，如不利用文件寄生(有的只存在于内存中)，对网络造成拒绝服务，以及和黑客技术相结合等。

普通病毒需要传播受感染的驻留文件来进行复制，而蠕虫不使用驻留文件即可在系统之间进行自我复制，普通病毒的传染能力主要是针对计算机内的文件系统而言，而蠕虫病毒的传染目标是互联网内的所有计算机。

1.1.3 木马

木马(Trojan Horse)，是从希腊神话里面的“特洛伊木马”得名的，希腊人在一只假装人祭礼的巨大木马中藏匿了许多希腊士兵并引诱特洛伊人将它运进城内，等到夜里马腹内士兵与城外士兵里应外合，一举攻破了特洛伊城。

而现在所谓的木马正是指那些表面上是有用的软件、实际目的却是危害计算机安全并导致严重破坏的计算机程序。它是具有欺骗性的文件(宣称是良性的，但事实上是恶意的)，是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。

所谓隐蔽性是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马，也难以确定其具体位置；所谓非授权性是指一旦控制端与服务端连接后，控制端将窃取到服务端的很多操作权限，如修改文件、修改注册表、控制鼠标和键盘、窃取信息等。一旦中了木马，系统可能就会门户大开，毫无秘密可言。

木马与病毒的重大区别是木马不具有传染性，它不能像病毒那样复制自身，也不“刻意”地去感染其他文件，它主要通过将自身伪装起来，吸引用户下载执行。特洛伊木马中包含能够在触发时导致数据丢失甚至被窃的恶意代码，要使特洛伊木马传播，必须在计算机上有效地启用这些程序，例如打开电子邮件附件或者将木马捆绑在软件中放到网络吸引人下载执行等。现在的木马一般主要以窃取用户相关信息为主要目的，相对病毒而言，可以简单地说，病毒破坏信息，而木马窃取信息。典型的特洛伊木马有“灰鸽子”、“网银大盗”等。

1.2 漏洞危害

1.2.1 生活中的安全问题

在2014年11月20日举行的网络空间安全和国际合作分论坛上，国家互联网应急中心主任黄澄清发表演讲指出，仅在2014年上半年，中国内地就有19万台机器感染了木马，其中美国通过木马程序控制了中国内地共计260万余台的主机，葡萄牙控制了241万台主机名列第二。

黑客是如何在主机中植入木马，达到入侵的目的？在回答这个问题之前，先介绍几个大家可能都遇到过的安全问题。

1. 重装系统后，刚连上网络就马上中毒

新买的计算机刚连上因特网才几天的时间，就发现计算机变得运行缓慢、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，最后的结果似乎连杀毒软件竟然也无法正常打开，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！

其实在判断自己的计算机中毒的时候，思路是正确的，然而再次中毒的时候，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，那么令人发狂的木马病毒程序又是从哪里进入计算机的呢？

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和防火墙软件，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。如果计算机安全用这样简单的方法就可以全面保护，那么怎么还能致使某某国家的政府计算机全部被恶意攻击造成瘫痪而损失惨重呢。这说明，计算机安全要比人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，人们使用的计算机其实就是计算机的俗称，一台计算机由硬件和软件两个部分组成，单纯地在计算机市场买到的就是计算机的硬件，人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暴露出来。即使暴露出来，它们也可能只会造成软件崩溃不能运行而已，通常称这些问题为软件的Bug。

可是，问题并非这么简单，软件中存在的一些问题可以在某种情况下被利用来对用户造成恶意攻击，如给用户计算机上安装木马病毒，或者直接盗取用户计算机上的秘密信息等。这个时候，软件的这些问题就不再是Bug，而是一个软件安全漏洞，简称软件漏洞。

上文中那种屡屡中毒的情况，在很大程度上就是因为计算机系统中的某个软件存在

安全漏洞，有人利用了这些漏洞来进行攻击，给计算机系统安装了木马病毒程序，所以杀毒软件、防火墙软件都无法阻止木马病毒的侵入。

如果服务器软件存在安全漏洞，或者系统中可以被 RPC 远程调用的函数中存在的缓冲区溢出漏洞，攻击者也可以发起“主动”进攻，这种情况，计算机会轻易沦为所谓的“肉鸡”。

2. 只是单击一个 URL 链接，并没有执行任何其他操作，为什么会中木马

如果浏览器在解析 HTML 文件时存在缓冲区溢出漏洞，那么攻击者就可以精心构造一个承载着恶意代码的 HTML 文件，并把链接发给用户。当用户单击这种链接时，漏洞被触发，从而导致 HTML 中所承载的恶意代码被执行。这段代码通常是在没有任何提示的情况下去指定的地方下载木马客户端并运行。

此外，第三方软件所加载的 ActiveX 控件中的漏洞也是被“网马”所经常利用的对象，所以千万不要忽视 URL 链接。

3. Word 文档、Power Point 文档、Excel 表格文档并非可执行文件，它们会导致恶意代码的执行吗

和 HTML 文件一样，这类文档本身虽然是数据文件，但是如果 Office 软件在解析这些数据文件的特定数据结构时存在缓冲区溢出漏洞，攻击者就可以通过一个精心构造的 Word 文档来触发并利用漏洞。当用户在用 Office 软件打开这个 Word 文档的时候，一段恶意代码可能已经悄无声息地被执行过了。

1.2.2 漏洞产业链

有多年使用经验的计算机用户可能有此类的感受。近年来，计算机被病毒感染导致无法运行、甚至需要重装的现象越来越少。在十几年前，正是病毒泛滥流行的时候，无论是熊猫烧香病毒，还是冲击波病毒，都迫使用户不得不反复重装电脑、经常扫描电脑，否则机器无法正常工作。是因为现在的 360 杀毒、百度杀毒等工具功能越来越强大了吗？还是因为现在制造病毒、木马的能力弱了？

在回答这个问题之前，有必要介绍一下目前的漏洞产业链。

20 世纪初，黑客是一个正义的名词，那个时候的黑客主要是致力于维护网络生态环境，将发现的错误报告给微软等公司。那个时候，很少有人炫耀自己攻击了什么网站，更不会有人想用网络技术非法牟利。那个时候，大家崇尚自由、共享的互联网精神，有一些心照不宣的网络道德标准。

而现在，良好生态逐渐被打破了。起先是一些公司出钱让黑客帮助寻找自己的安全漏洞，然后就发展为地下交易（中间人抢先把漏洞拿走，价格是公司的好几倍）。拿走漏洞有很多不可告人的商业用途。越来越多的黑客，已经把目光从率先发布漏洞的荣誉感转变为利用这些漏洞得到经济利益。

现在，全世界都有人找黑客提供服务，有些国家或政府也会向黑客购买信息，他们主要不是为了防堵安全漏洞，而是希望利用漏洞达成目的。泄露美国“棱镜”监控事件的斯诺登，在公布的机密文件中也揭露美国是程序漏洞的其中一个买主。

2011 年曾发生过黑客在网上公开了中国最大的开发者社区 CSDN 网站的用户数据库，600 多万个注册邮箱账号和与之对应的明文密码泄露。其实这些资料早就泄露了，已被用了好多次了。有人为了炫耀就公布了，随后陆续有人跟进，其实公开了就毫无利用价值。

这些靠漏洞赚钱的黑客，对网络环境的危害很大。他们惯用的手段一般有以下几种。

(1) 编写“免杀”木马。一旦游戏玩家中了这种木马病毒，账号和密码会自动发到一个地址里。他们还为木马程序进行“免杀升级”，这样一来，普通的杀毒软件就算及时更新升级，也无法查杀这个木马。一般都是用来盗取游戏账号卖钱。

(2) 偷流量。要么修改网站内的链接代码，当有人登录一些知名网站等次级链接时，会跳到其目标网站；或者在网站后台做手脚，当有人打开网站时，会自动暗中弹出其目标网站，用户却看不到。一些小网站靠广告赢利，广告商则按单击率给这些网站支付广告费。黑客在后台控制一些知名网站，可为客户瞬间提供几十万的单击率。因此，这些网站难免会遭受攻击。

(3) 商业间谍活动。有个黑客端着笔记本电脑进了一家酒店，第二天他出来的时候，电脑里存着这家酒店所有的客户数据。这是酒店竞争对手给他下的单子，为的是把客户都抢过来。这批数据卖了 100 多万元。还有一些公司在商业谈判前夕，请黑客去盗竞争对手的“底牌”。

(4) 通过网银偷钱。比这些更黑的生意是通过网银偷钱，但也更危险，很少有人敢在国内做。现在很多黑客把阵地从微软转到安卓、从电脑用户转到手机用户了。越来越多移动恶意程序拥有命令和控制服务器的后门。

1.2.3　漏洞产生的原因

1. 小作坊式的软件开发

严格地讲，任何一款计算机软件都必须依据软件工程的思想来进行设计开发。这是因为，软件工程是一种逻辑化很强的体系，它可以将软件需要的功能以及实现逻辑全部表现出来，开发人员只需要按照软件工程要求的具体步骤进行软件的代码编写，就可以完成软件的具体实现。这样开发出来的软件不但质量高，而且易于扩展与维护。

但是，出于种种原因，很多软件的开发并没有按照软件工程的要求来实现。因为进行软件工程开发需要有大量的金钱资本投入，一些小型的公司或者个人为了节约资金，就采用了直接开发，或者边设计边开发的方法，这样制作出来的软件犹如小作坊里生产出来的产品，质量参差不齐，难免存在很多的安全漏洞。

2. 赶进度带来的弊端

不是说按照软件工程开发出来的软件就一定不存在安全漏洞，很多大型的软件公司即使采用了软件工程思想来设计软件，但是由于时间紧迫，任务繁重，也会在一定程度上采用投机取巧或者偷工减料的办法来开发软件。这个时候开发出来的软件，往往由于开发者过于疲劳或者赶进度，从而将不安全的因素带进软件，造成软件存在安全漏洞。