

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
(第2版)

刘哲理 李进 贾春福 编著

<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

(第2版)

刘哲理 李进 贾春福 编著



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、信息安全专业应知应会的基础工具 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 Windows 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，目标是丰富基础知识和为 CTF 比赛提供技能储备，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 安全的知识等都值得一读。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。

版权所有，侵权必究。侵权举报电话：010-62782989 13701121933

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.—2版.—北京:清华大学出版社,2019
(高等院校信息安全专业系列教材)

ISBN 978-7-302-52704-6

I. ①漏… II. ①刘… ②李… ③贾… III. ①计算机网络—安全技术 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2019)第 063136 号

责任编辑：赵 凯

封面设计：常雪影

责任校对：胡伟民

责任印制：刘海龙

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 刷 者：北京富博印刷有限公司

装 订 者：北京市密云县京文制本装订厂

经 销：全国新华书店

开 本：185mm×260mm 印 张：15.5 字 数：385千字

版 次：2017年3月第1版 2019年8月第2版 印 次：2019年8月第1次印刷

定 价：59.00元

产品编号：083030-01

高等院校信息安全专业系列教材

编审委员会

顾问委员会主任：沈昌祥(中国工程院院士)

特别顾问：姚期智(美国国家科学院院士、美国人文及科学院院士、
中国科学院外籍院士、“图灵奖”获得者)

何德全(中国工程院院士) 蔡吉人(中国工程院院士)

方滨兴(中国工程院院士)

主任：肖国镇

副主任：封化民 韩 臻 李建华 王小云 张焕国

冯登国 方 勇

委员：(按姓氏笔画为序)

马建峰 毛文波 王怀民 王劲松 王丽娜

王育民 王清贤 王新梅 石文昌 刘建伟

刘建亚 许 进 杜瑞颖 谷大武 何大可

来学嘉 李 晖 汪烈军 吴晓平 杨 波

杨 庚 杨义先 张玉清 张红旗 张宏莉

张敏情 陈兴蜀 陈克非 周福才 宫 力

胡爱群 胡道元 侯整风 荆继武 俞能海

高 岭 秦玉海 秦志光 卿斯汉 钱德沛

徐 明 寇卫东 曹珍富 黄刘生 黄继武

谢冬青 裴定一

策划编辑：张 民

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知识的需求。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

当今人们已经身处互联网时代,在黑客入侵、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。

写这本书的目的就在于: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,提供一些解答。

如果想知道系统为什么不安全、黑客为什么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内容精髓,那就是如何编写安全的代码。代码审计和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,让互联网时代中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。

本教材第 1 版于 2017 年 3 月出版,得到广大读者喜爱,很快销售一空。笔者在实际授课过程中,进一步考虑到高校培养 CTF 人才需要,结合授课时的实际体会,在现有教材基础上进一步细分了知识点,增加了汇编基础、寻址方式、返回导向编程 ROP 技术、SQL 盲注、文件包含漏洞、反序列化漏洞以及整站攻击示例等内容,使得教材内容更加饱满,体系更加完整,作为一本网络安全攻防入门教材是很不错的。

刘哲理

2019 年 4 月

目 录

第 1 章 绪论	1
1.1 病毒和木马	1
1.1.1 病毒	1
1.1.2 蠕虫	2
1.1.3 木马	3
1.2 漏洞危害	3
1.3 渗透测试	7
1.4 实验环境	9
1.4.1 VMware Workstation 的使用	9
1.4.2 认识 Kali	11
第 2 章 基础知识	15
2.1 堆栈基础	15
2.1.1 内存区域	15
2.1.2 堆区和栈区	16
2.1.3 函数调用	16
2.1.4 常见寄存器与栈帧	18
2.2 汇编语言	20
2.2.1 主要寄存器	20
2.2.2 寻址方式	22
2.2.3 主要指令	24
2.2.4 函数调用汇编示例	26
2.3 二进制文件	30
2.3.1 PE 文件格式	30
2.3.2 虚拟内存	31
2.3.3 PE 文件与虚拟内存的映射	32
2.4 调试工具	34
2.4.1 OllyDBG	34
2.4.2 IDA	36
2.4.3 OllyDBG 示例	40

第3章 漏洞概念	45
3.1 概念及特点	45
3.1.1 概念	45
3.1.2 特点	46
3.2 漏洞分类	46
3.2.1 漏洞分类	46
3.2.2 危险等级划分	48
3.3 漏洞库	49
3.3.1 CVE	50
3.3.2 NVD	50
3.3.3 CNNVD	50
3.3.4 CNVD	51
3.3.5 BugTraq	51
3.3.6 其他漏洞库	51
3.4 第一个漏洞	52
3.4.1 漏洞示例	52
3.4.2 漏洞利用示例	54
第4章 常见漏洞	57
4.1 缓冲区溢出漏洞	57
4.1.1 基本概念	57
4.1.2 栈溢出漏洞	57
4.1.3 其他溢出漏洞	58
4.2 格式化字符串漏洞	63
4.3 整数溢出漏洞	67
第5章 漏洞利用	71
5.1 漏洞利用概念	71
5.1.1 有关概念	71
5.1.2 示例	72
5.1.3 Shellcode 编写	76
5.2 软件防护技术	79
5.2.1 ASLR	79
5.2.2 GS Stack protection	79
5.2.3 DEP	82
5.2.4 SafeSEH	82
5.2.5 SEHOP	83

5.3	漏洞利用技术	83
5.3.1	地址利用技术	83
5.3.2	绕过 DEP 保护	86
第 6 章	漏洞挖掘	89
6.1	静态检测	89
6.1.1	静态检测方法	89
6.1.2	静态安全检测技术的应用	91
6.1.3	静态安全检测技术的实践	91
6.2	动态检测	99
6.2.1	模糊测试	99
6.2.2	智能模糊测试	101
6.2.3	动态污点分析	102
6.2.4	动态检测实践	102
6.3	动静结合检测	109
第 7 章	渗透测试基础	111
7.1	渗透测试过程	111
7.2	Kali Linux 基础	114
7.2.1	常用指令	114
7.2.2	软件包管理	116
7.3	渗透测试框架	116
7.3.1	认识 Metasploit	116
7.3.2	常用命令	118
第 8 章	渗透测试实践	121
8.1	信息收集	121
8.1.1	被动信息收集	121
8.1.2	主动信息收集	125
8.2	扫描	130
8.2.1	Nessus 准备	130
8.2.2	Nessus 扫描	133
8.3	漏洞利用	135
8.4	后渗透攻击	139
8.4.1	挖掘用户名和密码	139
8.4.2	获取控制权	140

第9章 Web安全基础	143
9.1 基础知识	143
9.1.1 HTTP协议	143
9.1.2 HTML	143
9.1.3 JavaScript	144
9.1.4 HTTP会话管理	145
9.2 Web编程环境安装	146
9.2.1 环境安装	146
9.2.2 JavaScript实践	149
9.3 PHP与数据库编程	152
9.3.1 PHP语言	152
9.3.2 第一个Web程序	153
9.3.3 连接数据库	155
9.3.4 查询数据	156
9.3.5 一个完整的示例	156
9.3.6 Cookie实践	163
9.4 Web安全威胁	165
第10章 Web渗透实战基础	171
10.1 文件上传漏洞	171
10.1.1 WebShell	171
10.1.2 文件上传漏洞	172
10.2 跨站脚本攻击	177
10.2.1 脚本的含义	177
10.2.2 跨站脚本的含义	178
10.2.3 跨站脚本攻击的危害	180
10.3 SQL注入漏洞	185
10.3.1 SQL语法	185
10.3.2 注入原理	186
10.3.3 寻找注入点	187
10.3.4 SQLMap	189
10.3.5 SQL注入实践	189
10.3.6 SQL注入盲注	196
10.3.7 SQL注入防御措施	200
第11章 Web渗透实战进阶	202
11.1 文件包含漏洞	202
11.1.1 文件包含	202

11.1.2	本地文件包含漏洞	203
11.1.3	远程文件包含漏洞	204
11.1.4	PHP 伪协议	205
11.2	反序列化漏洞	207
11.2.1	序列化与反序列化	207
11.2.2	PHP 魔术方法	208
11.2.3	PHP 反序列化漏洞	209
11.3	整站攻击案例	212
第 12 章	软件安全开发	219
12.1	软件开发生命周期	219
12.1.1	软件开发生命周期	219
12.1.2	软件开发生命周期模型	220
12.2	软件安全开发	221
12.2.1	建立安全威胁模型	221
12.2.2	安全设计	222
12.2.3	安全编程	222
12.2.4	安全测试	223
12.3	软件安全开发生命周期	224
样题	229
参考文献	230

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，甚至区分不清什么是病毒，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。这三类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”。有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。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)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。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副本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)。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,胡乱吞食屏幕上的字母并将其形状改变。

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。

两个轰动全球的蠕虫病毒:

(1) 震网(Stuxnet)病毒。该病毒于2010年6月首次被检测出来,是第一个专门定向攻击真实世界中基础(能源)设施的“蠕虫”病毒,例如核电站、水坝、国家电网等。作为世界上首个网络“超级破坏性武器”,震网的计算机病毒已经感染了全球超过45 000个网络,伊朗遭到的攻击最为严重,其60%的个人电脑感染了这种病毒。由于震网感染的重灾区集中在伊朗境内。美国和以色列因此被怀疑是震网的发明人。这种新病毒采取了多种先进技术,因此具有极强的隐身和破坏力。只要电脑操作员将被病毒感染的U盘插入USB接口,这种病毒就会在神不知鬼不觉的情况下(不会有任何其他操作要求或者提示出现)取得一些工业用电脑系统的控制权。

(2) 比特币勒索(WannaCry)病毒。WannaCry又称为Wanna Decryptor,是一种“蠕虫式”的勒索病毒,在2017年5月份爆发。比特币勒索主要利用了微软“视窗”系统的漏洞,以获得自动传播的能力,能够在数小时内感染一个系统内的全部电脑。

被该勒索病毒入侵后,用户主机系统内的照片、图片、文档、音频、视频等几乎所有类型的文件都将被加密,加密文件的后缀名被统一修改为.WNCRY,并会在桌面弹出勒索对话框,要求受害者支付价值数百美元的比特币到攻击者的比特币钱包,且赎金金额还会随着时间的推移而增加。

该病毒由不法分子利用NSA(National Security Agency,美国国家安全局)泄露的危险漏洞EternalBlue(永恒之蓝)进行传播。勒索病毒肆虐,俨然是一场全球性互联网灾难,给广大电脑用户造成了巨大损失。最新统计数据 displays,100多个国家和地区超过10万台电脑遭到了比特币勒索病毒的攻击和感染。比特币勒索病毒全球大爆发时,至少150个国家、30万名用户中招,造成损失达80亿美元,已经影响到金融、能源、医疗等众多行业,造成严重的危机管理问题。在我国,部分Windows操作系统用户遭受感染,校园网用户首当其冲,受害严重,大量实验室数据和毕业设计被锁定加密,部分大型企业的系统和数据库文件被加密后,无法正常工作,影响巨大。

1.1.3 木马

木马(Trojan Horse)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。

木马是从希腊神话里面的“特洛伊木马”得名的,希腊人在一只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。

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。

此外,现在的木马一般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,病毒破坏你的信息,而木马窃取你的信息。

典型的特洛伊木马有灰鸽子、网银大盗等。

1.2

漏洞危害

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:重装系统后,刚连上网络就马上中毒。

新买的计算机刚连上网络才几天的时间,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也无法正常打开,便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。

1. 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,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。这些问题可能隐藏的很深,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缺陷(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(包括操作系统)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。

“电脑肉鸡”就是受别人控制的远程电脑。“肉鸡”可以是各种系统,如 Windows、Linux、UNIX 等;更可以是一家公司、企业、学校甚至是政府军队的服务器。如果服务器软件存在安全漏洞,攻击者可以发起“主动”进攻,植入木马,将该服务器变为一个任人宰割的“肉鸡”。

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,计算机就会轻易沦为所谓的“肉鸡”。

思考两个生活中的安全问题:

(1) 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。

(2) Word 文档、Power Point 文档、Excel 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。

2. 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,由于种种原因,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。

(3) 被轻视的软件安全测试。

按道理来讲,无论哪种模式开发出来的软件,既然是由人开发的,就很可能存在安全问题。为此,软件开发领域专门成立了软件安全测试这样一种机制来防止软件出现漏洞。

软件安全测试不但可以进行对软件代码的安全测试,还可以对软件成品进行安全测试。但是,对于一些开发商来说,这又会增加软件开发的成本。于是,他们要么不做软件安全测试,要做也就是最简单最低级的测试。他们只保证软件能够正常使用,基本功能都已实现,就觉得软件完美了,其实漏洞就这样被隐藏在了软件内部。

(4) 淡薄的安全思想。

安全思想主要是针对软件开发中最辛苦的编程人员来说的。由于编程人员对软件安全的认识并不一样,在做产品开发时,他们编写的代码也就对软件的安全出现了不同程度的影响。如果一个编程人员不具有一些基本的安全编程经验,他可能就会把最简单最常见的安全漏洞引入到软件内部。

不单单是编程人员,作为软件的整体设计者,在考虑软件的实现时,他很可能不考虑软件安全,而是一味地追求软件的功能实现、美工界面等。这样的安全思想就会导致软件出现这样或者那样的安全漏洞。