

网络攻防实战研究

漏洞利用与提权

祝烈煌 张子剑 主编
陈小兵 张胜生 王坤 徐焱 编著





网络攻防实战研究

漏洞利用与提权

祝烈煌 张子剑 主编
陈小兵 张胜生 王坤 徐焱 编著

电子工业出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书主要讨论目前常见的漏洞利用与提权技术，分别从攻击和防御的角度介绍渗透过程中相对最难，同时又是渗透最高境界的部分——如何获取服务器乃至整个网络的权限。本书共分9章，由浅入深，按照读者容易理解的方式对内容进行分类，每一节介绍一个典型应用，同时结合案例进行讲解，并给出一些经典的总结。本书的目的是介绍漏洞利用与提权技术，结合一些案例来探讨网络安全，从而远离黑客的威胁。通过本书的学习，读者可以快速了解和掌握主流的漏洞利用与提权技术，加固自己的服务器。

本书既可以作为政府、企业网络安全从业者的参考资料，也可以作为大专院校信息安全学科的教材。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

网络攻防实战研究：漏洞利用与提权 / 祝烈煌，张子剑主编；陈小兵等编著. —北京：电子工业出版社，2018.4

（安全技术大系）

ISBN 978-7-121-33240-1

I. ①网… II. ①祝… ②张… ③陈… III. ①计算机网络—网络安全—研究 IV. ①TP393.08

中国版本图书馆 CIP 数据核字（2017）第 306684 号

策划编辑：潘 昕

责任编辑：潘 昕

印 刷：三河市良远印务有限公司

装 订：三河市良远印务有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编：100036

开 本：787×1092 1/16 印张：41 字数：1150 千字

版 次：2018 年 4 月第 1 版

印 次：2018 年 4 月第 1 次印刷

定 价：128.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlbs@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）51260888-819，faq@phei.com.cn。

推荐序

在安全行业从业这么多年，回过头来发现，和小兵居然相识 10 年了。作为 10 年前就对网络安全有浓厚兴趣，在安全圈子里扎根、生长的技术人，小兵的自学能力和分享精神都是我所佩服的。

我一直认为，安全人才没有办法定向培养，只能依赖天赋，而我们要做的就是发掘和激发少部分人的天赋，最好的办法则是通过活生生的案例引发兴趣，让兴趣成为最好的导师。这本书也和小兵的为人一样实在，有大量干货、新货，能帮助刚对安全产生兴趣却不知道从哪里入手的读者快速入门、上手，通过本书捅破那层“窗户纸”，找到自己感兴趣的新领域。阅读本书，你将在网络安全的路上走得更快、更远！

360 网络攻防实验室负责人
陆羽（林伟）

在经典的渗透测试过程中，有很多行之有效的漏洞利用及相关场景下的提权思路，这本书对这些内容做了全面的介绍。这本书不仅覆盖攻击，还详细讲解了相应的防御方法，内容皆来自一线实战，值得参考。

《Web 前端黑客技术揭秘》作者
余弦

Shadow Brokers 发布“NSA 武器库”在网络世界所造成的影响，让我们感受到了“渗透之下，漏洞利用工具为王”的可怕。当漏洞利用工具并不完备时，网络渗透测试就无法有效地进行了吗？显然不是这样的。渗透的精髓在于组合与细节利用，在一万种网络系统环境中有一万种渗透思路和方法。这种极具创造性的“入侵”行为体现了渗透测试人员的能力与水平，经验老道的安全人员总有自己独特的“奇淫技巧”，这些技巧就像弹药一样，根据渗透目标的不同有的放矢，以最终获得目标高权限为结果的过程是有趣的且具有艺术性的。我想，这就是渗透测试的魅力所在。当一个安全人员通过别人从未尝试过的“组合拳”最终渗透了目标时，他所收获的成就感是无与伦比的。每个安全人员都对拥有大师级的网络渗透技术梦寐以求，而获得此水平的前提就在于基础一定要扎实，如果现在有一万种渗透技巧存在，那就将它们融会贯通，唯有消化和吸收了所有已知的渗透技巧，才能进一步缔造崭新的攻防手法。

本书是一本渗透技巧极其丰富的工具书，涵盖了渗透测试中绝大部分环境下的攻防利用之道，是初学者打基础、高手查缺补漏的绝佳教材。

360 独角兽安全团队创始人
杨卿

前 言

2017年5月15日爆发的WannaCry勒索病毒，中毒者欲哭无泪，全球损失惨重！通过此次事件，人们发现，网络安全不再遥远。以前提到“网络安全”“黑客”等字眼，人们大都会认为那是传说和传奇，一般都是一笑而过。而今，随着互联网攻防技术的发展，谁还能说自己在信息世界里可以独善其身？2016年雅虎泄露10亿条个人账号信息，国内被公开泄露的个人隐私数据甚至高达几十亿条。截至2017年年底，由于网络电信诈骗等导致的个人及公司损失超过100亿元。在科技飞速发展的今天，如果我们能掌握一些安全知识、提高自己的安全意识，就极有可能避免个人财产损失。

在2016年出版《黑客攻防：实战加密与解密》后，我们的团队经过一年多的努力，将全部研究成果分享给广大读者朋友。在本书中，我们从更加专业、更加体系化的角度来讨论和研究网络安全，对关键技术进行详细的研究、再现和总结，同时介绍了一些典型案例，让读者身临其境，充分了解和掌握漏洞利用与提权的精髓！

2017年6月1日，《中华人民共和国网络安全法》正式实施，国家对网络安全的重视程度前所未有，很多高校都新增或者加强了网络安全专业建设，将信息安全提升到一级学科，提升到国家战略层面！没有网络空间的安全，就没有国家的安全！

本书内容

本书主要讨论目前常见的漏洞利用和提权技术，从攻击与防御的角度介绍渗透过程中相对最难，同时又是渗透最高境界的部分——如何获取服务器乃至整个网络的权限。本书共分9章，由浅入深，按照读者容易理解的方式对内容进行分类，每一节介绍一个典型应用，同时结合案例进行讲解，并给出一些经典的总结。

第1章 提权基础

提权是整个黑客攻防过程中最难的环节，提权过程则汇聚了思路、技巧、工具和技术。本章着重介绍提权的基础知识，包括如何进行提权，如何破解Windows及Linux密码，一些后门工具的使用，如何实现对提权工具的免杀，以及端口转发和代理工具的使用。

第2章 Windows漏洞利用与提权

Windows是目前使用最为广泛的操作系统之一。从2000年开始，计算机操作系统飞速发展，从Windows 95到Windows Server 2017，人们感受到了互联网技术的跌宕起伏。在操作系统层面，曾经多次爆发高危漏洞，攻击者可以远程直接获取目标服务器的权限。在渗透过程中，很多人认为提权是最难攻克的，其实不然，只要掌握了相关的知识点，在各种技术的配合下，99%都可以提权成功。本章着重介绍Windows提权的基础知识、Windows提权技巧、常用的口令扫描方法及一些新颖的提权方法和思路。

第3章 Linux 漏洞利用与提权

在网络渗透过程中，经常碰到通过 CMS 等漏洞获取了服务器的 WebShell，但因为 Linux 服务器设置了严格的权限而较难获取 root 账号权限的情况。在本章中讨论了 Linux 密码的获取与破解，以及利用一些 Linux 漏洞来提权的方法和技巧。本章原来的设想是对 Linux 中存在的各种本地提权漏洞进行介绍和利用，但在实际测试过程中，未能达到大众化利用的程度，因此将在后续的图书中陆续介绍这些方法。本章将着重介绍如何对 Linux 密码进行破解，以及如何通过各种漏洞来渗透并提权 Linux 服务器。

第4章 MSSQL 漏洞利用与提权

MSSQL 数据库是微软开发的目前世界上最为流行的数据库软件之一，它只能运行在 Windows 平台上，最常见的架构为 ASP+MSSQL 和 ASP.NET+MSSQL。在 Windows Server 2008 以下版本中，只要获取了 sa 账号及其密码，就可以快速、方便地通过一些技巧获取系统权限。在 Windows Server 2008 以上版本中，虽然不能直接获取系统权限，但可以通过恢复存储过程等方式执行命令，通过系统中存在的提权漏洞进行提权。本章着重介绍 SQL Server 提权的基础知识，以及 Windows 下 SQL Server 的提权方法，同时通过一些案例介绍了如何利用 sa 账号来提权。

第5章 MySQL 漏洞利用与提权

MySQL 数据库是目前世界上最为流行的数据库软件之一，很多流行的架构都会用到 MySQL，例如 LAMP (Linux+Apache+MySQL+PHP+Perl) 架构。目前很多流行的 CMS 系统使用 MySQL+PHP 架构，MySQL 主要在 Windows 和 Linux 操作系统中安装使用。因此，在获取了 root 账号的情况下，攻击者通过一些工具软件和技巧极有可能获取系统的最高权限。本章着重介绍 MySQL 提权的基础知识，以及 Windows 下 MySQL 的提权方法，同时通过一些案例介绍了如何利用 MySQL 来提权。

第6章 Oracle 漏洞利用与提权

Oracle 是一款大型的数据库系统，市场占有率很高，在数据库领域有极其重要的地位。作为世界上第一个支持 SQL 语言的关系型数据库，Oracle 提供了丰富的包和存储过程，支持 Java 和创建 library 等特性，拥有丰富的系统表，几乎所有的信息都存储在系统表里，包括当前数据库运行的状态、用户的信息、数据库的信息、用户所能访问的数据库和表的信息等，在提供强大功能的同时，也带来了众多隐患。从第一代 Oracle 产品发布起，互联网上就不断有 Oracle 数据库的安全漏洞被公开。虽然 Oracle 一直在努力弥补这些缺陷，例如定期发布更新补丁去修复已发现的安全漏洞，但是随着 Oracle 数据库版本的更新，新的漏洞层出不穷。此外，由于数据库管理员安全意识较弱或未进行全面、有效的安全策略配置，导致数据库存在被攻击的安全风险。对 Oracle 的攻击主要包括弱口令或默认口令的猜解、SQL 注入、权限配置不当、拒绝服务攻击等。本章针对 Oracle 数据库漏洞介绍了常见的提权方法及相应的防御手段。

第7章 Metasploit 漏洞利用与提权

在 Metasploit 下所说的提权，通常是指在已经获得 MSF 的 Meterpreter Shell 后采取的各种提升权限的方法。通常，在渗透过程中很有可能只获得了一个系统的 Guest 或 User 权限的 Meterpreter Shell，如果在网络环境中仅获得受限用户权限，那么在实施横向渗透或者提权攻击时将很困难。在主机上，如果没有管理员权限，就无法进行获取 Hash 值、安装软件、修改防火墙规则和修改注册表等操作，所以，必须将访问权限从 Guest 提升到 User，再到 Administrator，最后到 System 级别。可

以说，渗透的目的是获取服务器的最高权限，即 Windows 操作系统中管理员账号的权限或 Linux 操作系统中 root 账户的权限。

第 8 章 其他应用程序漏洞利用与提权

在本章主要介绍一些应用程序的提权，包括 Serv-U、Winmail、Radmin、pcAnywhere、JBoss、Struts、JspRun、Gene6 FTP Server、Tomcat、Citrix、VNC、ElasticSearch、Zabbix 等。

第 9 章 Windows 及 Linux 安全防范

本章就一些常见的系统漏洞和弱点进行分析。真正的安全防范是一个持续的改进和完善过程，我们需要随时关注 0day 及安全漏洞。在网络攻防过程中，安全防范非常重要：攻击方需要隐藏自己的 IP 地址、消除痕迹、防止被发现；而防守方则关注如何加固，如何使自己的系统更安全，“牢不可破”是终极目标。在武侠小说中经常提及一个理念：最好的防御就是攻击。通过攻击自身系统发现漏洞，对漏洞进行分析、修补和加固，也就有了日常听到的安全公司进行某项目的安全评估。

虽然本书内容已经比较丰富和完整了，但仍然无法涵盖所有的漏洞利用与提权技术。通过本书的学习，读者可以快速了解和掌握主流的漏洞利用与提权渗透技术，加固自己的服务器。本书的目的是介绍漏洞利用与提权技术，结合一些案例来探讨网络安全，帮助读者更好地加固服务器，远离黑客的威胁。

资源下载

书中提到的所有资源的下载地址为 <http://pan.baidu.com/s/1slGynDj>，密码为 41ne。

特别声明

本书是安全帮（www.secbang.com）定制的培训教材，同时被部分高校列为指定教材。本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任。本书的目的是最大限度地唤醒读者对网络安全的重视，并采取相应的安全措施，从而减少由网络安全漏洞带来的经济损失。

由于笔者水平有限，加之时间仓促，书中疏漏之处在所难免，恳请广大读者批评指正。

反馈与提问

在阅读本书的过程中，如果读者遇到问题或有任何意见，都可以发邮件至 antian365@gmail.com 与笔者直接联系。

致谢

本书主编是祝烈煌、张子剑。参加本书编写工作的有陈小兵、张胜生、王坤、徐焱、刘晨、黄小波、韦亚奇、邓火英、刘漩、庞香平、武师、陈尚茂、邱永永、潘喆、孙立伟、陈海华、邓北京、兰云碧、易金云、吴海春。

感谢电子工业出版社对本书的大力支持，尤其是潘昕编辑为本书出版所做的大量工作，感谢美编对本书进行的精美的设计。借此机会，还要感谢多年来在信息安全领域给我教诲的所有良师益友，感谢众多热心网友对本书的支持。最后要感谢家人，是他们的支持和鼓励使本书得以顺利完成。

另外，本书集中了北京理工大学多位老师和安天 365 团队众多“小伙伴”的智慧。我们的团队

是一个低调潜心研究技术的团队。衷心地感谢团队成员夏洛克、雨人、imiyoo、cnbird、Xnet、fido、指尖的秘密、Leoda、pt007、Mickey、YIXIN、终隐、fivestars、暖色调の微笑、304、Myles等，是你们给了我力量，给了我信念。最后，还要特别感谢安全圈的好友范渊、孙彬、罗诗尧、杨卿、杨哲、杨文飞、林伟、余弦、王亚智、傅烨文、汤志强、菲哥哥、张健、-273.15℃、风宁、杨永清、毕宁、韩晨、叶猛、刘璇，是你们的鼓励、支持和建议让本书更加完美。

编 者

2018年1月于北京

目 录

第 1 章 提权基础	1	1.5.1 简介	30
1.1 提权概述	1	1.5.2 使用方法	31
1.1.1 提权简介	1	1.5.3 参数详解	31
1.1.2 提权条件	2	1.5.4 使用实例	32
1.1.3 提权准备工作	2	1.5.5 总结与思考	33
1.1.4 实施提权	4	1.6 对提权工具 PR 的免杀	34
1.2 Windows 账号和密码的获取与破解	6	1.6.1 什么是 PR	34
1.2.1 使用 GetHashes 获取 Windows 系统密码 Hash 值	6	1.6.2 如何对提权工具进行免杀	34
1.2.2 使用 gsecdump 获取 Windows 系统密码	7	1.6.3 加壳软件 VMProtect Ultimate	37
1.2.3 使用 PwDump 获取域控密码	9	1.7 通过 LCX 端口转发实现内网突破	39
1.2.4 使用 PwDump 获取系统账号和密码	11	1.7.1 确定被控制计算机的 IP 地址	39
1.2.5 使用 SAMInside 获取及破解 Windows 系统密码	12	1.7.2 在被控制计算机上执行端口转发命令	40
1.2.6 使用 oclHashcat 破解 Windows 系统账号密码	13	1.7.3 在本机上执行监听命令	40
1.2.7 使用 L0phtCrack 破解 Windows 及 Linux 密码	16	1.7.4 在本机上使用远程终端进行登录	41
1.2.8 使用 Ophcrack 破解系统 Hash 密码	20	1.7.5 查看本地连接	41
1.3 使用 John the Ripper 破解 Linux 密码	25	1.8 使用 SocksCap 进行内网突破	42
1.3.1 准备工作	25	1.8.1 安装并运行 SocksCap	42
1.3.2 John 的 4 种破解模式	26	1.8.2 设置 SocksCap	43
1.3.3 使用 John 破解 Linux 密码	26	1.8.3 建立应用程序标识项	43
1.3.4 查看破解结果	28	1.8.4 运行“命令行”代理	44
1.4 Linux 提权辅助工具 Linux Exploit Suggester	28	1.8.5 总结与思考	44
1.4.1 列出可能的漏洞	28	1.9 Windows 系统提权基础命令	44
1.4.2 下载可利用的脚本	30	1.9.1 获取 IP 地址信息	44
1.4.3 编译并执行	30	1.9.2 获取端口信息	45
1.4.4 总结与思考	30	1.9.3 获取服务信息和进程信息	45
1.5 PHP WeBaCoo 后门	30	1.9.4 进程结束命令	46
		1.9.5 用户管理命令	47
		1.9.6 开启 3389 端口	48
		第 2 章 Windows 漏洞利用与提权	49
		2.1 Windows 提权基础	49
		2.1.1 Windows 提权信息的收集	50

2.1.2	Windows 提权准备	52	2.8.2	实战 MS08-067 远程漏洞利用	95
2.1.3	使用 MSF 平台搜索可利用的 POC	53	2.8.3	防范措施	102
2.1.4	实施提权	54	2.9	通过 Pr 提权渗透某高速服务器	102
2.1.5	相关资源	54	2.9.1	分析 AWS 扫描结果	102
2.1.6	Windows 本地溢出漏洞及对应版本	55	2.9.2	获取 WebShell	103
2.1.7	停用安全狗	58	2.9.3	服务器信息收集与 Pr 提权	104
2.2	提权辅助工具 Windows-Exploit-Suggester	58	2.10	以 Public 权限渗透某 ASP.NET 网站	110
2.2.1	Windows-Exploit-Suggester 简介	58	2.10.1	寻找漏洞并进行渗透测试	110
2.2.2	使用 Windows-Exploit-Suggester	59	2.10.2	寻找、测试和获取 WebShell	113
2.2.3	技巧与高级利用	60	2.10.3	尝试提权	116
2.3	Windows 低权限进程及服务提权	65	2.10.4	使用 lcx 命令转发并登录远程桌面	116
2.3.1	AccessChk 简介及使用	65	2.10.5	总结与思考	118
2.3.2	获取低权限可操作服务的名称	66	2.11	Windows 7/2008 服务器 64 位版本 MS12-042 漏洞提权	118
2.3.3	修改服务并获取系统权限	68	2.11.1	MS12-042 漏洞简介	118
2.4	Windows 口令扫描及 3389 口令暴力破解	70	2.11.2	提权工具	118
2.4.1	口令扫描准备工作	70	2.11.3	实战提权利用	119
2.4.2	使用 NTscan 扫描口令	71	2.12	对某虚拟主机的一次 SiteManager 提权	121
2.4.3	使用 Tscrack 扫描 3389 口令	75	2.12.1	获取虚拟主机某站点的 WebShell	121
2.4.4	使用 Fast RDP Brute 暴力破解 3389 口令	79	2.12.2	使用 WebShell 中的提权功能尝试提权	122
2.5	使用 WinlogonHack 获取系统密码	81	2.12.3	查看可写目录	122
2.5.1	远程终端密码泄露分析	81	2.12.4	渗透成功	124
2.5.2	WinlogonHack 截取密码原理	81	2.12.5	继续渗透内外网	126
2.5.3	使用 WinlogonHack 获取密码实例	82	2.13	社工渗透并提权某服务器	127
2.5.4	攻击与防范方法探讨	83	2.13.1	网站挂马的检测和清除	127
2.5.5	自动获取并发送密码到指定网站	85	2.13.2	入侵痕迹的搜索和整理	129
2.6	Windows Server 2003 域控服务器密码获取	86	2.13.3	利用社会工程学进行反渗透	129
2.6.1	域控服务器渗透思路	87	2.14	通过 SQL 注入漏洞渗透某服务器并直接提权	132
2.6.2	内网域控服务器渗透常见命令	87	2.14.1	对目标站点的分析和漏洞利用	132
2.6.3	域控服务器用户账号和密码获取实例	88	2.14.2	尝试提权获取管理员权限	134
2.7	MS05-039 漏洞利用实战	92	2.15	phpinfo 函数信息泄露漏洞的利用与提权	135
2.7.1	MS05-039 漏洞简介	92	2.15.1	phpinfo 函数简介	135
2.7.2	实战 MS05-039 漏洞利用	93	2.15.2	phpinfo 函数信息泄露漏洞	135
2.8	MS08-067 远程溢出漏洞利用实战	95			
2.8.1	MS08-067 漏洞描述	95			

2.15.3 通过 phpinfo 函数信息泄露漏洞 渗透获取 WebShell 权限	136
2.15.4 服务器提权	138
2.15.5 总结与思考	139
2.16 通过简单的漏洞渗透某公司 内外部网络	140
2.16.1 测试页面漏洞的检测	140
2.16.2 测试页面漏洞的利用思路	140
2.16.3 登录服务器并进行口令扫描	142
2.16.4 获取域控密码	142
2.16.5 测试页面漏洞的修复	143
2.17 通过文件上传漏洞渗透某 Windows 2012 服务器并提权	143
2.17.1 初步渗透	143
2.17.2 获取 WebShell	145
2.17.3 使用 WebShell 进行提权并 登录服务器	146
2.17.4 总结与思考	146
2.18 通过戴尔服务器远程访问管理卡 获取服务器权限	148
2.18.1 获取服务器远程访问管理卡 的账号和密码	148
2.18.2 加载 ISO 文件	149
2.18.3 替换文件获取服务器权限	150
第 3 章 Linux 漏洞利用与提权	151
3.1 使用 fakesu 记录 root 用户的密码	151
3.1.1 使用 kpr-fakesu.c 记录 root 用户 的密码	151
3.1.2 运行键盘记录程序	153
3.1.3 查看密码记录文件	154
3.1.4 删除安装文件	155
3.2 使用 Hydra 暴力破解 Linux 密码	155
3.2.1 Hydra 简介	155
3.2.2 Hydra 的安装与使用	156
3.2.3 Hydra 应用实例	158
3.3 Linux 操作系统 root 账号密码获取 防范技术研究	162
3.3.1 Linux 密码原理	162
3.3.2 Linux 系统采用的加密算法	163
3.3.3 获取 Linux root 密码方法研究	164
3.3.4 Linux root 账号密码防范技术	167
3.4 通过 Linux OpenSSH 后门获取 root 密码	167
3.4.1 OpenSSH 简介	167
3.4.2 准备工作	168
3.4.3 设置 SSH 后门的登录密码及其 密码记录位置	169
3.4.4 安装并编译后门	170
3.4.5 登录后门并查看记录的密码文件	170
3.4.6 拓展密码记录方式	171
3.4.7 OpenSSH 后门的防范方法	172
3.4.8 总结	173
3.5 利用 FCKeditor 漏洞渗透某 Linux 服务器	174
3.5.1 对已有 WebShell 进行分析和研究	175
3.5.2 测试上传的 WebShell	177
3.5.3 分析与收集 WebShell 所在 服务器的信息	177
3.5.4 服务器提权	179
3.6 chkrootkit 0.49 本地提权漏洞利用 与防范研究	181
3.6.1 漏洞分析	181
3.6.2 漏洞利用条件	182
3.6.3 实际测试	183
3.6.4 漏洞利用扩展	183
3.6.5 漏洞利用与防范方法探讨	184
3.7 从服务器信息泄露到 Linux 服务器 权限获取	185
3.7.1 服务器信息泄露的危害	185
3.7.2 服务器信息泄露的获取	185
3.7.3 服务器信息泄露的利用	186
3.7.4 服务器信息泄露渗透实例	186
3.8 通过 WinSCP 配置文件获取 Linux 服务器权限	188
3.8.1 发现主站 SQL 注入漏洞并 获取 WebShell	189
3.8.2 发现弱口令	190

3.8.3 进入主站所在服务器及相关服务器	191	3.13.5 Linux 下的快速渗透思路	209
3.8.4 总结	193	3.13.6 相关源代码	210
3.9 通过网上信息获取某 Linux 服务器 权限	193	3.13.7 利用 s02-045 漏洞快速渗透 某服务器	212
3.9.1 通过 SSH 账号和密码进行 登录测试	193	3.14 安全设置 Linux 操作系统的密码	214
3.9.2 成功登录 Linux 服务器	194	3.14.1 修改 login.defs 中的参数	215
3.9.3 查看服务器文件及所有信息	194	3.14.2 设置加密算法	215
3.9.4 查看服务器所在 IP 地址下网站的 域名情况	195	3.14.3 破解 Linux 密码	215
3.9.5 尝试获取 WebShell	195	第 4 章 MSSQL 漏洞利用与提权	217
3.9.6 总结与思考	195	4.1 SQL Server 提权基础	217
3.10 渗透某 Linux 服务器并提权	196	4.1.1 SQL Server 简介	217
3.10.1 收集网站基本信息	196	4.1.2 sa 口令的获取	218
3.10.2 扫描端口开放情况	197	4.1.3 常见 SQL Server 提权命令	218
3.10.3 漏洞扫描和测试	197	4.1.4 通过数据库备份获取 WebShell	222
3.10.4 服务器提权	197	4.1.5 SQL Server 日志	223
3.11 通过 SQL 注入获取某 Linux 服务器 权限	198	4.2 SQL Server 口令扫描	223
3.11.1 漏洞扫描与利用	198	4.2.1 使用 Piggy 进行口令扫描	224
3.11.2 获取 Linux 账号和密码	200	4.2.2 使用 SQLPing 进行口令扫描	225
3.11.3 破解 Linux 账号	200	4.2.3 使用 Hscan 扫描 MSSQL 口令	226
3.11.4 获取 Linux SSH 账号权限	201	4.3 SQL Server 2000 MS08-040 漏洞	227
3.11.5 总结与思考	201	4.3.1 使用 MySQLSrv 8.0.194 AutoAttack 进行扫描并渗透	228
3.12 Struts 2 远程代码执行漏洞 s2-032 及其提权利用	202	4.3.2 获取反弹 Shell 并继续渗透	229
3.12.1 Struts 简介	202	4.3.3 登录服务器远程终端	231
3.12.2 s2-032 漏洞简介	202	4.3.4 总结与思考	232
3.12.3 漏洞测试样例	202	4.4 SQL Server 2000 提权	233
3.12.4 网上公开的检测地址	204	4.4.1 SQL 版本号查询	233
3.12.5 网上公开的 s2-032 漏洞综合 利用工具	204	4.4.2 通过查询分析获取管理员权限	234
3.12.6 s2-032 漏洞的利用及提权	204	4.4.3 通过手工注入点获取管理员权限	234
3.13 快速利用 s02-45 漏洞获取 服务器权限	206	4.4.4 恢复存储过程	235
3.13.1 CVE-2017-5638 漏洞简介	206	4.4.5 SQL server 提权防范方法	237
3.13.2 漏洞实际利用	206	4.5 SQL Server 2005 提权	237
3.13.3 修改 POC 利用代码	207	4.5.1 查看数据库连接文件	237
3.13.4 在 Windows 下快速实施渗透	208	4.5.2 获取数据库用户和密码	238
		4.5.3 数据库连接设置	238
		4.5.4 查看连接信息	238
		4.5.5 添加 xp_cmdshell 存储过程	239
		4.5.6 添加用户	240

4.5.7 将普通用户添加到管理员组	240	第 5 章 MySQL 漏洞利用与提权	264
4.5.8 通过 XP_cmdshell exec 查看系统用户	241	5.1 MySQL 提权基础	264
4.5.9 远程终端登录	241	5.1.1 MySQL 提权必备条件	265
4.5.10 总结	241	5.1.2 MySQL 密码获取与破解	265
4.6 Windows Server 2008 中 SQL Server 2008 的提权	242	5.1.3 通过 MySQL 获取 WebShell	267
4.6.1 SQL Server 2008 提权思路	242	5.1.4 MySQL 渗透技巧总结	267
4.6.2 获取 SQL Server 2008 sa 账号密码	242	5.2 用 MOF 方法提取 MySQL root 权限	271
4.6.3 恢复存储过程并查看和读取磁盘文件	243	5.2.1 漏洞利用方法分析	272
4.6.4 生成并获取 WebShell	244	5.2.2 实战利用	273
4.6.5 上传并获取 JSP WebShell	245	5.2.3 防范方法	276
4.6.6 获取系统密码并登录服务器	246	5.3 MySQL 数据库 UDF 提权	276
4.7 通过 Windows Server 2008 和 SQL Server 2008 sa 权限获取 WebShell	246	5.3.1 UDF 函数简介	276
4.7.1 以 sa 权限获取 WebShell 的思路	246	5.3.2 Windows 下 UDF 提权的条件和方法	277
4.7.2 利用实例	247	5.3.3 提权实例	279
4.7.3 防范建议	250	5.3.4 其他提权工具	282
4.8 通过 sa 权限注入获取服务器权限	250	5.3.5 UDF 提权总结与防范	283
4.8.1 获取漏洞并进行测试	250	5.4 通过 MySQL 数据库反弹端口连接提权	284
4.8.2 Windows 提权	252	5.4.1 反弹端口连接提权的条件	284
4.8.3 信息收集及其他渗透	253	5.4.2 实现方法	285
4.8.4 总结与思考	255	5.4.3 提权实例	285
4.9 通过 FTP 账号渗透并提权某服务器	255	5.4.4 防范方法	287
4.9.1 通过扫描获取 FTP 权限	255	5.5 通过 MySQL 账号社工渗透某 Linux 服务器	287
4.9.2 获取 WebShell	256	5.5.1 漏洞发现及测试	287
4.9.3 获取数据库账号和密码	256	5.5.2 利用已有信息渗透 MySQL 数据库	288
4.9.4 数据库服务器直接提权	257	5.5.3 进行社工攻击	290
4.9.5 总结与思考	259	5.5.4 总结与探讨	291
4.10 Windows Server 2003 下 SQL Server 2005 绕过安全狗提权	259	5.6 MySQL root 口令的利用及提权	291
4.10.1 通过扫描获取口令	259	5.6.1 分析及利用漏洞	292
4.10.2 基本信息收集	259	5.6.2 获取 WebShell	293
4.10.3 添加管理员提权失败	260	5.6.3 服务器提权	295
4.10.4 寻求突破	260	5.7 从 MySQL 口令扫描到提权	296
4.10.5 绕过安全狗的其他方法	263	5.7.1 通过扫描获取 root 口令	296
4.10.6 总结	263	5.7.2 进行提权	298

5.7.3 总结与思考	301	6.1.5 Oracle 默认账号及密码	330
5.8 MySQL 无法通过 WebShell 执行命令 提权某服务器	301	6.2 Oracle 口令破解	330
5.8.1 获取数据库 root 密码	301	6.2.1 利用 Metasploit 暴力猜解 Oracle 数据库	331
5.8.2 获取 WebShell	301	6.2.2 利用 odat 暴力猜解 Oracle 数据库	333
5.8.3 无法执行命令	301	6.2.3 利用 Orabrute 暴力猜解 Oracle 数据库	335
5.8.4 使用反弹端口提权	302	6.2.4 通过数据库配置文件获取 Oracle 口令	336
5.8.5 总结与思考	305	6.3 通过注入存储过程提升数据库 用户权限	338
5.9 phpMyAdmin 漏洞利用与安全防范	306	6.3.1 原理介绍	338
5.9.1 MySQL root 账号密码获取思路	306	6.3.2 手工注入 SYS.DBMS_CDC_ SUBSCRIBE.ACTIVATE _SUBSCRIPTION 提升权限	338
5.9.2 获取网站真实路径的思路	307	6.3.3 利用 Metasploit 实施注入	341
5.9.3 MySQL root 账号 WebShell 获取思路	308	6.4 Web 下的 SQL 注入及提权	342
5.9.4 无法通过 phpMyAdmin 直接 获取 WebShell	310	6.4.1 SQL 注入攻击基础知识	342
5.9.5 phpMyAdmin 漏洞防范方法	311	6.4.2 利用超级 SQL 注入工具实施 SQL 注入	344
5.10 巧用 Cain 破解 MySQL 数据库密码	311	6.4.3 利用 sqlmap 实施 SQL 注入	345
5.10.1 MySQL 加密方式	312	6.4.4 利用 utl_http.request 存储过程 实施反弹注入攻击	346
5.10.2 MySQL 数据库文件结构	313	6.4.5 利用 dbms_xmlquery.newcontext() 函数进行服务器提权	347
5.10.3 获取 MySQL 数据库用户密码 加密字符串	313	6.5 在 Oracle 上利用 Java 执行命令	349
5.10.4 将 MySQL 用户密码字符串 加入 Cain 破解列表	314	6.5.1 原理介绍	349
5.10.5 使用字典进行破解	315	6.5.2 在 Oracle 11g 上利用 Java 执行命令	350
5.10.6 总结与思考	316	6.5.3 在 Oracle 10g 上利用 Java 执行命令	351
5.11 MySQL 数据库安全加固	319	6.6 利用 SQL*Plus 获取 WebShell	353
5.11.1 补丁安装	319	6.6.1 原理介绍	353
5.11.2 账户密码设置	320	6.6.2 获取 WebShell	353
5.11.3 匿名账户检查	320	6.7 Oracle 数据库备份	355
5.11.4 数据库授权	321	6.7.1 利用 exp 备份数据库	355
5.11.5 网络连接设置	321	6.7.2 利用 PL/SQL Developer 备份数据	356
5.11.6 文件安全设置	322	6.7.3 利用 JSP 脚本备份数据库	356
第 6 章 Oracle 漏洞利用与提权	324		
6.1 Oracle 提权基础	324		
6.1.1 Oracle 的安装	325		
6.1.2 Oracle 管理工具	327		
6.1.3 Oracle 权限介绍	329		
6.1.4 PL/SQL 介绍	330		

6.8 Oracle 数据库攻击的防范方法.....	358
6.8.1 数据库安全纵深防御.....	359
6.8.2 部署数据库防火墙.....	360
第 7 章 Metasploit 漏洞利用与提权.....	362
7.1 Metasploit 提权基础知识.....	363
7.1.1 Metasploit 简介.....	363
7.1.2 Metasploit 基础.....	364
7.1.3 后渗透工具 Meterpreter.....	364
7.2 PowerShell 渗透利用剖析.....	365
7.2.1 PowerShell 的基本概念.....	366
7.2.2 PowerShell 的基本设置和常用命令.....	366
7.2.3 PowerShell 下常用的攻击工具.....	368
7.3 getsystem 提权全解析.....	372
7.3.1 查询当前权限.....	372
7.3.2 使用 getsystem 命令提权.....	373
7.4 MS16-016 本地溢出漏洞利用实战.....	374
7.4.1 MS16-016 漏洞提权简介.....	374
7.4.2 Metasploit 下 MS16-016 漏洞 提权实战.....	374
7.4.3 修复方式.....	377
7.5 通过 WMIC 实战 MS16-032 溢出漏洞.....	377
7.5.1 WMIC 简介.....	377
7.5.2 MS16-032 漏洞简介.....	378
7.5.3 Metasploit 下 MS16-032 漏洞 提权实战.....	378
7.5.4 PowerShell 下 Invoke-MS16-032 脚本提权实战.....	381
7.6 绕过用户控制实战.....	383
7.6.1 UAC 简介.....	383
7.6.2 利用 bypassuac 绕过 UAC 实战演练.....	383
7.6.3 利用 RunAs 绕过 UAC 实战演练.....	385
7.7 通过假冒令牌获取 Windows Server 2008 R2 域管权限.....	386
7.7.1 令牌简介.....	386
7.7.2 关于令牌的一些问题.....	386
7.7.3 令牌的工作机制.....	387
7.7.4 Metasploit 下假冒令牌提权实战.....	387
7.8 错误的 Windows 系统配置漏洞 提权实战.....	389
7.8.1 Trusted Service Paths 漏洞介绍.....	390
7.8.2 Trusted Service Paths 漏洞产生原因.....	390
7.8.3 Metasploit 下 Trusted Service Paths 漏洞利用实战.....	390
7.8.4 系统服务错误权限配置漏洞简介.....	392
7.8.5 PowerUp 对系统服务错误权限 配置漏洞的利用.....	393
7.9 Windows 服务漏洞研究与利用.....	396
7.9.1 Windows 服务漏洞介绍.....	396
7.9.2 Windows 服务漏洞利用实战.....	396
7.10 AlwaysInstallElevated 提权 实战演练.....	399
7.10.1 Windows Installer 相关知识介绍.....	399
7.10.2 AlwaysInstallElevated 简介.....	399
7.10.3 Metasploit 下 AlwaysInstallElevated 提权实战演练.....	399
7.10.4 PowerShell 下 AlwaysInstall Elevated 提权实战演练.....	402
7.10.5 AlwaysInstallElevated 漏洞 产生原因.....	403
7.11 Metasploit 下 Mimikatz 的使用.....	404
7.11.1 Mimikatz 简介.....	404
7.11.2 Mimikatz 的使用.....	404
7.12 通过 Metasploit 渗透手机.....	407
7.12.1 生成反弹木马.....	408
7.12.2 监控手机实测.....	409
7.13 移植 s2-045 漏洞利用代码模块实战.....	411
7.13.1 s2-045 漏洞简介.....	411
7.13.2 s2-045 漏洞的原理.....	411
7.13.3 s2-045 漏洞的危害及修复措施.....	412
7.13.4 移植 s2-045 漏洞利用代码模块.....	412
7.13.5 Metasploit 下 s2-045 漏洞 提权实战.....	413
第 8 章 其他应用程序漏洞利用与提权.....	415
8.1 通过 Serv-U 提权 ASP.NET 服务器.....	415

8.1.1 利用 WebShell 查看系统管理员 用户组	416	8.6.3 通过 JBoss 信息泄露获取 WebShell	457
8.1.2 执行 SU Exp	416	8.7 Struts s2-016 和 s2-017 漏洞 利用实例	461
8.1.3 检查 Serv-U 提权情况	417	8.7.1 搜寻目标站点	461
8.1.4 远程终端登录测试	418	8.7.2 测试网站能否正常访问	462
8.1.5 总结与思考	419	8.7.3 测试 Struts2 s2-016 漏洞	462
8.2 扫描 FTP 口令并利用 Serv-U 提权 某服务器	419	8.7.4 获取 WebShell 权限	463
8.2.1 信息收集	420	8.7.5 总结与思考	463
8.2.2 口令检测	420	8.8 从 JspRun 后台获取 WebShell	465
8.2.3 实施控制和渗透	422	8.8.1 进入系统后台	465
8.2.4 内网渗透和查看	424	8.8.2 新增模板	466
8.2.5 简单的安全加固	427	8.8.3 在模板中创建文件	467
8.2.6 总结与思考	428	8.8.4 测试并访问 Shell	467
8.3 Windows Server 2008 中的 Magic Winmail Server 提权	429	8.8.5 JspRun 论坛的其他相关漏洞	468
8.3.1 获取 Winmail 目录地址	429	8.8.6 总结与思考	469
8.3.2 执行 whoami 命令	429	8.9 Gene6 FTP Server 本地提权	469
8.3.3 添加用户到管理员组	430	8.9.1 通过互联网获取漏洞的利用信息	469
8.3.4 设置并登录远程终端服务器	430	8.9.2 修改 user 配置参数获取本地 服务器权限	470
8.3.5 Winmail 邮箱用户与口令	431	8.9.3 漏洞修复和加固方法	472
8.3.6 进入邮箱	431	8.10 通过 Tomcat 弱口令提取某 Linux 服务器权限	472
8.3.7 Winmail 服务器安全防范	432	8.10.1 使用 Apache Tomcat Crack 暴力破解 Tomcat 口令	472
8.4 Radmin 网络渗透提权研究	432	8.10.2 部署 WAR 格式的 WebShell	473
8.4.1 Radmin 简介	432	8.10.3 获取系统加密的用户密码	475
8.4.2 Radmin 口令暴力攻击	433	8.10.4 总结与思考	477
8.4.3 Radmin 在渗透中的妙用	435	8.11 Citrix 密码绕过漏洞引发的渗透	478
8.4.4 利用 Radmin 口令进行内网 渗透控制	439	8.11.1 Citrix 简介	478
8.4.5 利用 Radmin 口令进行外网 渗透控制	441	8.11.2 Citrix 的工作方式	478
8.4.6 远程控制软件 Radmin 提权研究	442	8.11.3 Citrix 渗透实例	478
8.5 pcAnywhere 账号和口令的破解 与提权	445	8.11.4 总结与思考	482
8.5.1 pcAnywhere 账号和口令破解	446	8.12 从 CuteEditor 漏洞利用到全面 控制服务器	482
8.5.2 一个渗透实例	447	8.12.1 初步的安全渗透测试	482
8.6 JBoss 远程代码执行漏洞提权	454	8.12.2 旁注渗透测试	485
8.6.1 JBoss 远程代码执行漏洞利用	454	8.12.3 通过 CuteEditor 上传获得突破	488
8.6.2 JBoss 远程代码执行漏洞防范方法	457	8.12.4 提升权限	491

8.12.5 安全建议和总结	494	8.17.5 Zabbix 服务器的安全检查	528
8.13 利用 VNC 认证口令绕过漏洞 进行渗透	494	8.17.6 漏洞修复方案	529
8.13.1 扫描开放 5900 端口的计算机	495	8.18 OpenSSL “心脏出血” 漏洞分析 及利用	529
8.13.2 整理开放 5900 端口的 IP 地址	496	8.18.1 漏洞分析	530
8.13.3 整理扫描批处理命令	497	8.18.2 可利用 POC 及其测试	531
8.13.4 使用 VNC 连接器 Link 进行连接	497	8.18.3 OpenSSL 检测技术	534
8.13.5 处理连接结果	498	8.18.4 漏洞修复建议	536
8.13.6 实施控制	498	8.19 ImageMagick 远程执行漏洞 分析及利用	537
8.13.7 总结与思考	499	8.19.1 ImageMagick 远程执行漏洞分析	537
8.14 Oday 分析之 ColdFusion 本地 包含漏洞的利用方法	499	8.19.2 可利用 POC 测试	537
8.14.1 搭建 Goldfusion 测试平台	499	8.19.3 总结与思考	539
8.14.2 Oday 使用方法测试	500	8.19.4 防范方法	540
8.14.3 LFI to Shell in ColdFusion 6-10 利用方法分析	502	8.20 Linux glibc 幽灵漏洞的测试 与修复	540
8.14.4 其他可供利用 Oday 的分析	502	8.20.1 Linux glibc 幽灵漏洞测试方法	541
8.15 Elasticsearch 命令执行漏洞利用 及渗透提权	504	8.20.2 POC 验证测试	542
8.15.1 CVE-2015-1427 Groovy 命令 执行漏洞	504	8.20.3 修复方法	544
8.15.2 CVE-2014-3120 MVEL 命令 执行漏洞	505	第 9 章 Windows 及 Linux 安全防范	545
8.15.3 获取 Windows Server 2012 权限	505	9.1 网站挂马的检测与清除	546
8.15.4 通过 perl 反弹 Shell	507	9.1.1 检测网页木马程序	546
8.15.5 通过 Elasticsearch Groovy 可 执行命令漏洞获取某网站 WebShell 权限	510	9.1.2 清除网站中的恶意代码 (挂马代码)	550
8.16 通过 JBoss Application Server 获取 WebShell	513	9.2 巧用 MBSA 检查和加固个人计算机	551
8.16.1 扫描 JBoss Application Server 端口	514	9.2.1 实验准备和环境	552
8.16.2 通过 JBoss AS 部署 WebShell	516	9.2.2 使用 MBSA 检测和加固系统	552
8.16.3 获取 JSP 的 WebShell	519	9.2.3 总结与思考	557
8.17 Zabbix SQL 注入漏洞及利用探讨	520	9.3 使用冰刀、Antorun、CurrPorts 等 工具进行安全检查	557
8.17.1 Zabbix SQL 注入漏洞简介	520	9.3.1 使用冰刀进行安全检查	557
8.17.2 漏洞原理分析	520	9.3.2 使用 autoruns 进行安全检查	560
8.17.3 漏洞实际利用方法探讨	526	9.3.3 使用 CurrPorts 进行端口安全检查	563
		9.3.4 使用 FPort 与 MPort 进行端口 安全检查	564
		9.3.5 使用 Process Explorer 进行 安全清理	566
		9.4 巧用事件查看器维护服务器安全	568