Broadview®
www.broadview.com.cn

安全技术大系

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

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

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

電子工業出版社
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。

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 zlts@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 LAMPP（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 Guset 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