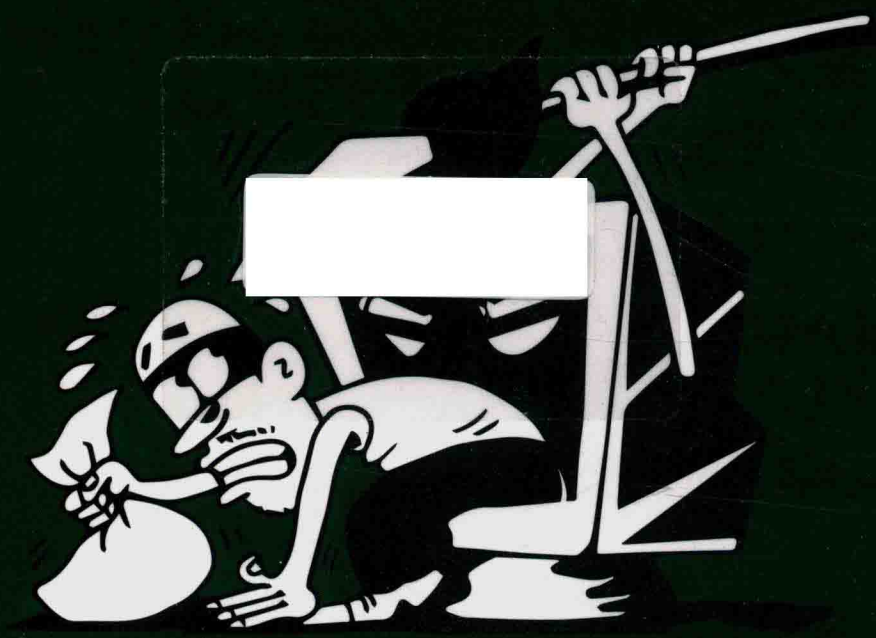
Broadview
www.broadview.com.cn

安全技术大系

实战案例分析Web渗透中的密码保护
在攻防中更好地保护网站和系统

黑客攻防
实战加密与解密

陈小兵　刘晨　黄小波　编著



结合网络攻防中的实际案例
系统、全面地介绍密码的防护与破解
图文并茂地再现Web渗透涉及的密码获取与破解过程

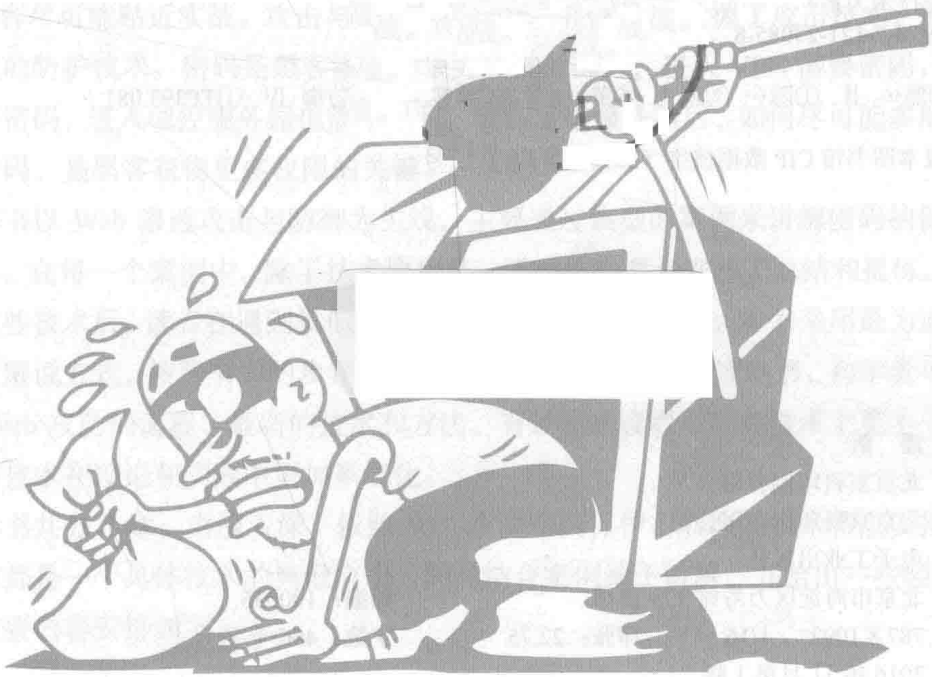
中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

黑客攻防

实战加密与解密

陈小兵　刘晨　萧小波　编著



電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书从黑客攻防的专业角度，结合网络攻防中的实际案例，图文并茂地再现 Web 渗透涉及的密码获取与破解过程，是市面上唯一一本对密码获取与破解进行全面研究的图书。本书共分 7 章，由浅入深地介绍和分析了目前流行的 Web 渗透攻击中涉及的密码获取、密码破解方法和手段，并结合多年的网络安全实践经验给出了相对应的安全防范措施，对一些经典案例还给出了经验总结和技巧。本书最大的特色就是实用和实战性强，思维灵活，内容主要包括 Windows 操作系统密码的获取与破解、Linux 操作系统密码的获取与破解、数据库密码的获取与破解、电子邮件密码的获取与破解、无线网络密码的获取与破解、App 密码的获取与破解、各种应用软件的密码破解、破解 WebShell 口令、嗅探网络口令、自动获取远程终端口令等。

本书既可以作为政府、企业相关人员研究网络安全的参考资料，也可以作为大专院校学生学习渗透测试的教材。

图书在版编目（CIP）数据

黑客攻防：实战加密与解密 / 陈小兵，刘晨，黄小波编著. —北京：电子工业出版社，2016.11
（安全技术大系）
ISBN 978-7-121-29985-8

Ⅰ. ①黑… Ⅱ. ①陈… ②刘… ③黄… Ⅲ. ①黑客－网络防御 Ⅳ. ①TP393.081

中国版本图书馆 CIP 数据核字（2016）第 233632 号

责任编辑：潘　昕
印　　刷：北京京科印刷有限公司
装　　订：北京京科印刷有限公司
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：22.75　　字数：466 千字
版　　次：2016 年 11 月第 1 版
印　　次：2016 年 11 月第 1 次印刷
定　　价：69.00 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。

前　言

在出版《黑客攻防实战案例解析》、《Web 渗透技术及实战案例解析》和《安全之路——Web 渗透技术及实战案例解析（第 2 版）》后，我和安天 365 团队经过讨论，决定将技术进行细化，进行专题研究，编写一系列黑客攻防实战方面的图书。经过近一年的努力，终于将《黑客攻防：实战加密与解密》完成。

本书从 Web 渗透的专业角度系统探讨黑客安全攻防中涉及的密码获取与破解技术，内容尽可能贴近实战。攻击与防护是辩证统一的关系，掌握了攻击技术，也就掌握了相应的防护技术。密码是黑客渗透中最为关键的部分，进入 VPN 需要密码，进入邮箱需要密码，进入域控服务器也需要密码。在渗透进服务器后，如何尽可能多地搜集和获取密码，是黑客获得更多权限的关键。

本书以 Web 渗透攻击与防御为主线，主要通过典型的案例来讲解密码的保护和破解技术。在每一个案例中，除了技术原理外，还对技术要点进行了总结和提炼。掌握和理解这些技术后，读者在遇到类似的场景时可以自己进行操作。本书采用最为通俗易懂的图文解说方式，按照书中的步骤即可还原攻防情景。通过阅读本书，初学者可以很快掌握 Web 攻防的流程、最新的技术和方法，有经验的读者可以在技术上更上一层楼，让攻防技术在理论和实践中更加系统化。

本书共分 7 章，由浅入深，依照 Web 攻防密码保护与获取的技术特点安排内容，每一节都是一个具体技术的典型应用，同时结合案例给予讲解，并给出一些经验总结。本书主要内容安排如下。

第 1 章　Windows 操作系统密码的获取与破解

介绍目前黑客攻防过程中如何获取 Windows 操作系统的密码，如何使用 LC5、Ophcrack、Hashcat 等工具对获取系统密码 Hash 值进行快速破解，以及如何安全设置操作系统的密码和如何检查系统是否存在克隆账号等。

第 2 章 Linux 操作系统密码的获取与破解

介绍 Linux 操作系统 root 账号和密码的获取与破解，使用 fakesu 记录 root 用户密码，Hydra 暴力破解密码，读取 Linux 保存的密码等。

第 3 章 数据库密码的获取与破解

介绍常见的数据库加密方式，破解 Access 密码，破解 MySQL 数据库密码，通过网页文件获取数据库账号和口令，扫描获取 SQL Server 肉机，通过 sa 权限、MySQL root 提权等。

第 4 章 电子邮件密码的获取与破解

电子邮箱是存储私密和敏感信息的重要位置。本章主要介绍如何快速获取浏览器中保存的邮箱和网站等的密码，如何获取 Foxmail 等软件保存的密码，以及如何扫描和攻击邮箱口令等，并给出了相应的防范建议。

第 5 章 无线网络密码的获取与破解

介绍如何使用 CDlinux 无线破解系统破解无线网络的密码，如何获取系统保存的无线网络密码，以及如何利用公共无线网络密码渗透并获取他人的邮箱口令等。

第 6 章 App 密码的获取与破解

本章介绍如何对 App 程序进行反编译并获取程序中的密码等信息，同时对手机木马反编译、手机锁等技术进行了探讨。

第 7 章 其他密码的获取与破解

本章主要介绍 pcAnywhere、VNC 等账号和口令的破解，讨论 Discuz! 论坛密码记录及安全验证问题暴力破解、一句话密码破解获取网站 WebShell，以及使用 Burp Suite 破解 WebShell 密码、手工检测黑客工具“中国菜刀”是否包含后门等。

虽然本书内容已经比较丰富和完整，但仍然无法涵盖所有的黑客攻防技术。技术的探索没有止境，更多的工具和方法，读者可以在日常学习和工作中去探索和发现。

资源下载

笔者在书中提到的所有相关资源可以到安天 365 网站（http://www.antian365.com）下载。特别是作者在多年工作中收集的渗透工具包，也在安天 365 网站免费提供下载。

特别声明

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。本书的目的在于最大限度地唤醒大家对网络安全的重视，并采取相应的安全措施，从而减少由网络安全问题带来的经济损失。

由于作者水平有限，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

读者在阅读本书过程中遇到任何问题或者有任何意见，都可以直接发电子邮件至antian365@gmail.com 进行反馈。

读者也可以加入 Web 安全图书交流 QQ 群（436519159）进行交流。

致谢

参加本书编写工作的有陈小兵、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。

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。感谢美工对本书进行的精美设计。

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。

最后要感谢我的家人，是他们的支持和鼓励使本书得以顺利完成。

本书集中了安全 365 团队众多“小伙伴”的智慧。我们是一个低调潜心研究技术的团队，我衷心地向团队的所有成员表示感谢，感谢雨人、Cold、imiyoo、cnbird、pt007、Mickey、Xnet、fido、指尖的秘密、Leoda、pt007、Mickey、YIXIN、终隐、fivestars、暖色调の微笑、幻想弦乐、Unsafe、雄究究、gh0stbo、人海孤鸿、LCCL 等，是你们给了我力量，给了我信念。

作　者

2016 年 3 月于北京

目　录

第 1 章　Windows 操作系统密码的获取与破解 1

1.1　使用 GetHashes 获取 Windows 系统密码 2
1.1.1　Hash 的基础知识 2
1.1.2　Windows 的 Hash 密码值 3
1.1.3　使用 GetHashes 获取 Windows 的 Hash 密码值 7
1.1.4　使用 GetHashes 获取系统 Hash 值的技巧 9
1.2　使用 gsecdump 获取 Windows 系统密码 9
1.2.1　下载和使用 gsecdump 10
1.2.2　gsecdump 参数 10
1.2.3　使用 gsecdump 获取系统密码 11
1.3　使用 Quarks PwDump 获取域控密码 11
1.3.1　使用 Quarks PwDump 获取本地账号的 Hash 值 12
1.3.2　使用 Quarks PwDump 导出账号实例 12
1.3.3　配合使用 NTDSutil 导出域控密码 13
1.4　使用 PwDump 获取系统账号和密码 14
1.4.1　上传文件到欲获取密码的计算机 14
1.4.2　在 Shell 中执行获取密码的命令 14
1.4.3　通过 LC5 导入 SAM 文件 15
1.4.4　破解系统账号和密码 16
1.4.5　破解结果 16
1.5　使用 SAMInside 获取及破解 Windows 系统密码 18
1.5.1　下载和使用 SAMInside 18
1.5.2　使用 Scheduler 导入本地用户的 Hash 值 19
1.5.3　查看导入的 Hash 值 19
1.5.4　导出系统用户的 Hash 值 20
1.5.5　设置 SAMInside 的破解方式 20
1.5.6　执行破解 21
1.6　Windows Server 2003 域控服务器用户账号和密码的获取 22
1.6.1　域控服务器渗透思路 22
1.6.2　内网域控服务器渗透的常见命令 22
1.6.3　域控服务器用户账号和密码获取实例 25
1.7　使用 Ophcrack 破解系统 Hash 密码 29
1.7.1　查找资料 29
1.7.2　配置并使用 Ophcrack 进行破解 32
1.7.3　彩虹表破解密码防范策略 37
1.8　使用 oclHashcat 破解 Windows 系统账号和密码 38
1.8.1　准备工作 39
1.8.2　获取并整理密码 Hash 值 39
1.8.3　破解 Hash 值 41

1.8.4 查看破解结果 42
1.8.5 小结 42
1.9 使用 L0phtCrack 破解 Windows 和 Linux 的密码 42
1.9.1 破解本地账号和密码 42
1.9.2 导入 Hash 文件进行破解 44
1.9.3 Linux 密码的破解 46
1.10 通过 hive 文件获取系统密码 Hash 48
1.10.1 获取 SAM、System 及 Security 的 hive 文件 48
1.10.2 导入 Cain 工具 49
1.10.3 获取明文密码 49
1.10.4 破解 Hash 密码 50
1.10.5 小结 51
1.11 使用 Fast RDP Brute 破解 3389 口令 51
1.11.1 Fast RDP Brute 简介 51
1.11.2 设置主要参数 52
1.11.3 局域网扫描测试 52
1.11.4 小结 53
1.12 Windows 口令扫描攻击 53
1.12.1 设置 NTscan 54
1.12.2 执行扫描 55
1.12.3 实施控制 56
1.12.4 执行 psexec 命令 57
1.12.5 远程查看被入侵计算机的端口开放情况 57
1.12.6 上传文件 58
1.12.7 查看主机的基本信息 59
1.13 使用 WinlogonHack 获取系统密码 59
1.13.1 远程终端密码泄露分析 60
1.13.2 WinlogonHack 获取密码的原理 60
1.13.3 使用 WinlogonHack 获取密码实例 62
1.13.4 WinlogonHack 攻击与防范方法探讨 63
1.13.5 使用 WinlogonHack 自动获取密码并发送到指定网站 65
1.14 检查计算机账号克隆情况 67
1.14.1 检查用户 68
1.14.2 检查组 68
1.14.3 使用 Mt 进行检查 69
1.14.4 使用本地管理员检测工具进行检查 70
1.15 安全设置操作系统的密码 70
1.15.1 系统密码安全隐患与现状 71
1.15.2 系统密码安全设置策略 72
1.15.3 系统密码安全检查与防护 75

第 2 章 Linux 操作系统密码的获取与破解 77

2.1 使用 fakesu 记录 root 用户的密码 77
2.1.1 使用 kpr-fakesu.c 程序记录 root 用户的密码 77
2.1.2 运行前必须修改程序 78
2.1.3 运行键盘记录程序 79
2.2 暴力破解工具 Hydra 82
2.2.1 Hydra 简介 82
2.2.2 Hydra 的安装与使用 82
2.2.3 Hydra 使用实例 85
2.3 Linux 操作系统 root 账号密码的获取 89
2.3.1 Linux 密码的构成 90
2.3.2 Linux 密码文件的位置 91
2.3.3 Linux 系统采用的加密算法 91
2.3.4 获取 Linux root 密码的方法 92
2.3.5 暴力破解法 94
2.3.6 Linux root 账号密码破解防范技术 95
2.3.7 小结 96
2.4 安全设置 Linux 操作系统的密码 97
2.4.1 修改 login.defs 中的参数 97
2.4.2 设置加密算法 97
2.4.3 破解 Linux 密码 98
2.5 Linux OpenSSH 后门获取 root 密码 99
2.5.1 OpenSSH 简介 100
2.5.2 准备工作 100
2.5.3 设置 SSH 后门的登录密码及其密码记录位置 102

2.5.4 安装并编译后门 103
2.5.5 登录后门并查看记录的密码文件 104
2.5.6 拓展密码记录方式 104
2.5.7 OpenSSH 后门的防范方法 107
2.5.8 小结 107

第 3 章 数据库密码的获取与破解 109

3.1 Discuz! 论坛密码记录及安全验证问题暴力破解 109
3.1.1 Discuz! 论坛密码记录程序的编写及实现 110
3.1.2 Discuz! X2.5 密码安全问题 111
3.1.3 Discuz! X2.5 密码安全问题的暴力破解 112
3.2 Access 数据库破解实战 114
3.2.1 Access 数据库简介 114
3.2.2 Access 数据库密码破解实例 116
3.3 巧用 Cain 破解 MySQL 数据库密码 117
3.3.1 MySQL 的加密方式 118
3.3.2 MySQL 数据库文件结构 119
3.3.3 破解 MySQL 数据库密码 120
3.3.4 破解探讨 123
3.4 MD5 加密与解密 127
3.4.1 MD5 加解密知识 128
3.4.2 通过 cmd5 网站生成 MD5 密码 128
3.4.3 通过 cmd5 网站破解 MD5 密码 128
3.4.4 通过在线 MD5 破解网站付费破解高难度的 MD5 密码 129
3.4.5 使用字典暴力破解 MD5 密码值 129
3.4.6 一次破解多个密码 132
3.4.7 MD5 变异加密的破解 133
3.5 MD5（Base64）加密与解密 134
3.5.1 MD5（Base64）密码简介 134
3.5.2 在网上寻找破解之路 135
3.5.3 寻求解密方法 135
3.5.4 探寻 MD5（Base64）的其他破解方式 138
3.5.5 MD5（Base64）原理 140
3.5.6 小结 141
3.6 通过网页文件获取数据库账号和口令 141
3.6.1 确认网站脚本类型 142
3.6.2 获取网站目录位置 143
3.6.3 查看网页脚本并获取数据库连接文件 143
3.6.4 获取数据库用户账号和密码等信息 144
3.6.5 实施控制 144
3.6.6 防范措施 145
3.6.7 小结 145
3.7 SQL Server 2000 口令扫描 145
3.7.1 设置 Hscan 146
3.7.2 查看扫描结果 147
3.7.3 连接数据库 148
3.7.4 执行命令 148
3.7.5 执行其他控制命令 149
3.7.6 小结 149
3.8 MySQL 口令扫描 149
3.8.1 设置 Hscan 150
3.8.2 查看扫描结果 150
3.8.3 连接并查看数据库服务器中的数据库 151
3.8.4 创建表并将 VBS 脚本插入表 151
3.8.5 将 VBS 脚本导出到启动选项中 152
3.8.6 等待重启和实施控制 154
3.8.7 小结 155
3.9 巧用 Cain 监听网络获取数据库口令 155
3.9.1 安装和配置 Cain 155
3.9.2 查看 Sniffer 结果 155
3.9.3 直接获取系统中有关保护存储的账号和密码 156
3.9.4 查看数据库密码 157
3.9.5 小结 157

3.10 MySQL 数据库提权 157
3.10.1 设置 MySQL 提权脚本文件 ... 157
3.10.2 进行连接测试 158
3.10.3 创建 shell 函数 158
3.10.4 查看用户 159
3.10.5 创建具有管理员权限的用户 ... 159
3.10.6 提权成功 160
3.10.7 小结 161
3.11 SQL Server 数据库的还原 162
3.11.1 SQL Server 2005 的新特性 162
3.11.2 还原和备份 SQL Server 2005 数据库 164
3.11.3 SQL Server 2008 数据库还原故障解决 169
3.12 SQLRootKit 网页数据库后门控制 172
3.12.1 使用 SQLRootKit 1.0 网页后门控制计算机 172
3.12.2 使用 SQLRootKit 3.0 网页后门控制计算机 173
3.12.3 防范措施 175
3.12.4 小结 176
3.13 SQL Server 2005 提权 176
3.13.1 查看数据库连接文件 176
3.13.2 获取数据库用户和密码 177
3.13.3 数据库连接设置 177
3.13.4 查看连接信息 178
3.13.5 添加 xp_cmdshell 存储过程 178
3.13.6 Windows 本地提权 179
3.13.7 小结 181

第 4 章 电子邮件密码的获取与破解 182

4.1 Foxmail 6.0 密码获取与嗅探 182
4.1.1 使用“月影”软件获取 Foxmail 6.0 密码及邮件资料 183
4.1.2 使用 Cain 软件获取 Foxmail 账号和密码 184
4.1.3 小结 185
4.2 使用 Hscan 扫描 POP3 口令 186
4.2.1 设置 Hscan 186
4.2.2 查看扫描结果 186
4.2.3 登录 Webmail 邮件服务器 186
4.2.4 查看邮件 187
4.2.5 口令扫描安全解决方案 187
4.2.6 小结 188
4.3 使用 Mail PassView 获取邮箱账号和口令 188
4.3.1 通过 Radmin 远程获取邮箱账号和密码 188
4.3.2 通过远程终端获取邮箱账号和密码 189
4.4 使用 Mailbag Assistant 获取邮件内容 190
4.4.1 恢复邮件内容的一些尝试 190
4.4.2 使用 Mailbag Assistant 恢复邮件内容 192
4.4.3 邮件内容防查看措施 195
4.4.4 小结 195
4.5 电子邮件社会工程学攻击和防范 196
4.5.1 社会工程学 196
4.5.2 常见的电子邮件社会工程学攻击方法 197
4.5.3 电子邮件社会工程学攻击的步骤 198
4.5.4 电子邮件社会工程学攻击的防范方法 199
4.5.5 小结 200
4.6 使用 IE PassView 获取网页及邮箱密码 200
4.6.1 IE PassView 简介 201
4.6.2 获取保存的网页及邮箱密码 201
4.6.3 对获取的信息进行处理 202
4.6.4 小结 202
4.7 Chrome 浏览器存储密码获取技术及防范 202
4.7.1 使用 WebBrowserPassView 获取浏览器密码 203
4.7.2 通过编写程序获取 Chrome 浏览器保存的密码 204
4.7.3 浏览器密码获取的防范方法 207

4.8 使用 EmailCrack 破解邮箱口令 208
4.8.1 通过邮件账号获取 SMTP 服务器地址 208
4.8.2 运行 EmailCrack 209
4.8.3 设置字典 209
4.8.4 破解邮件账号 210
4.8.5 小结 210

第 5 章 无线网络密码的获取与破解 211

5.1 使用 CDlinux 轻松破解无线网络密码 211
5.1.1 准备工作 211
5.1.2 开始破解 212
5.1.3 破解保存的握手包文件 213
5.2 使用 WirelessKeyView 轻松获取无线网络密码 215
5.2.1 WirelessKeyView 简介 215
5.2.2 使用 WirelessKeyView 获取无线网络密码 215
5.2.3 小结 217

第 6 章 App 密码的获取与破解 219

6.1 手机 APK 程序编译攻略 219
6.1.1 准备工作 220
6.1.2 使用 ApkTool 反编译 apk 221
6.1.3 使用 dex2jar 反编译 apk 222
6.1.4 使用 smali 反编译 apk 223
6.2 Android 手机屏幕锁解锁技术 224
6.2.1 Android 屏幕锁的分类 224
6.2.2 图案锁定及解锁 224
6.2.3 PIN 和密码锁定及解锁 226
6.2.4 更多解锁方法 228
6.3 钓鱼网站 APK 数据解密与分析 229
6.3.1 收集手机木马文件 229
6.3.2 分析手机木马程序 230
6.3.3 编写自动提取木马敏感信息的程序 231
6.4 对一款手机木马的分析 233
6.4.1 对手机短信进行分析 233
6.4.2 对 APK 进行反编译和追踪 235
6.4.3 手机 APK 安全防范 238

第 7 章 其他类型密码的获取与破解 240

7.1 pcAnywhere 账号和口令的破解 241
7.1.1 在本地查看远程计算机是否开放了 5631 端口 241
7.1.2 查找 pcAnywhere 账号和密码文件 241
7.1.3 将 CIF 加密文件传输到本地并进行破解 242
7.1.4 连接 pcAnywhere 服务端 242
7.2 使用 Router Scan 扫描路由器密码 243
7.2.1 运行 Router Scan 2.47 243
7.2.2 设置 Router Scan 扫描参数 244
7.2.3 查看并分析扫描结果 246
7.3 使用 ZoomEye 渗透网络摄像头 247
7.3.1 摄像头常见漏洞分析 247
7.3.2 实战演练 249
7.3.3 防范措施及建议 251
7.4 Discuz! 管理员复制提权技术 252
7.4.1 Discuz! 论坛的加密方式 252
7.4.2 使用 MySQL-Front 管理 MySQL 数据库 254
7.4.3 实施管理员复制 256
7.4.4 管理员密码丢失解决方案 257
7.4.5 小结与探讨 260
7.5 RAR 加密文件的破解 260
7.5.1 设置 Advanced RAR Password Recovery 260
7.5.2 使用字典文件进行破解 261
7.5.3 使用暴力破解方式破解密码 262
7.5.4 小结 263
7.6 一句话密码破解获取某网站 WebShell 263
7.6.1 获取后台权限 264
7.6.2 尝试提权 264
7.6.3 列目录及文件漏洞 265

7.6.4 一句话密码破解.....265
7.6.5 获取目标 WebShell 权限.....266
7.6.6 小结.....266
7.7 使用 Burp Suite 破解 WebShell 密码.....266
7.7.1 应用场景.....267
7.7.2 安装与设置.....267
7.7.3 破解 WebShell 的密码.....268
7.8 Radmin 远控口令攻防全攻略.....272
7.8.1 Radmin 简介.....272
7.8.2 Radmin 的基本操作.....273
7.8.3 Radmin 的使用.....279
7.8.4 Radmin 口令暴力破解.....282
7.8.5 Radmin 在渗透中的妙用.....285
7.8.6 利用 Radmin 口令进行内网渗透控制.....290
7.8.7 利用 Radmin 口令进行外网渗透控制.....293
7.9 通过扫描 Tomcat 口令渗透 Linux 服务器.....296
7.9.1 使用 Apache Tomcat Crack 暴力破解 Tomcat 口令.....296
7.9.2 对扫描结果进行测试.....296
7.9.3 部署 WAR 格式的 WebShell.....297
7.9.4 查看 Web 部署情况.....297
7.9.5 获取 WebShell.....298
7.9.6 查看用户权限.....298
7.9.7 上传其他 WebShell.....299
7.9.8 获取系统加密的用户密码.....299
7.9.9 获取 root 用户的历史操作记录.....300
7.9.10 查看网站域名情况.....300
7.9.11 获取网站的真实路径.....301
7.9.12 保留 WebShell 后门.....301
7.9.13 小结.....302
7.10 VNC 认证口令绕过漏洞攻击.....302
7.10.1 扫描开放 5900 端口的计算机.....303
7.10.2 整理开放 5900 端口的 IP 地址.....304
7.10.3 整理扫描批处理命令.....305
7.10.4 使用 VNC 连接器 Link 进行连接.....305
7.10.5 处理连接结果.....306
7.10.6 实施控制.....307
7.10.7 小结.....308
7.11 Serv-U 密码破解.....308
7.11.1 获取 ServUDaemon.ini 文件.....308
7.11.2 查看 ServUDaemon.ini 文件.....309
7.11.3 破解 Serv-U 密码.....310
7.11.4 验证 FTP.....311
7.12 使用 Cain 嗅探 FTP 密码.....312
7.12.1 安装 Cain.....312
7.12.2 设置 Cain.....312
7.12.3 开始监听.....313
7.12.4 运行 FTP 客户端软件.....313
7.12.5 查看监听结果.....314
7.12.6 小结.....315
7.13 利用 Tomcat 的用户名和密码构建后门.....315
7.13.1 检查 Tomcat 设置.....316
7.13.2 查看 Tomcat 用户配置文件.....317
7.13.3 进入 Tomcat 管理.....318
7.13.4 查看部署情况.....318
7.13.5 部署 JSP WebShell 后门程序.....319
7.13.6 测试后门程序.....319
7.13.7 在 WebShell 中执行命令.....320
7.13.8 防范措施.....321
7.13.9 小结.....321
7.14 破解静态加密软件.....321
7.14.1 软件注册方式.....321
7.14.2 破解实例.....322
7.15 Word 文件的加密与解密.....327
7.15.1 加密 Word 文件.....327
7.15.2 破解加密的 Word 文件.....328
7.16 Citrix 密码绕过漏洞引发的渗透.....331
7.16.1 Citrix 简介.....331
7.16.2 Citrix 的工作方式.....331
7.16.3 Citrix 渗透实例.....331

7.16.4　问题与探讨.....336
7.17　从渗透扫描到路由器跳板攻击.....337
7.17.1　渗透准备.....337
7.17.2　渗透扫描和连接测试.....337
7.17.3　跳板思路的测试和验证.....339
7.17.4　路由器攻击和测试.....341
7.17.5　加固方法.....342
7.18　手工检测“中国菜刀”是否包含后门.....342
7.18.1　“中国菜刀”简介.....343
7.18.2　实验环境.....343
7.18.3　分析并获取后门.....343
7.18.4　小结.....347
7.19　FlashFXP 密码的获取.....347
7.19.1　修改设置.....348
7.19.2　查看并获取密码.....348
7.19.3　查看 quick.dat 文件.....349

第 1 章　Windows 操作系统密码的获取与破解

Windows 操作系统是目前世界上最为流行的、使用最为广泛的操作系统之一，由于操作简单、实用、方便等特点，深受个人计算机用户喜爱。也正因如此，Windows 是最易受到攻击的操作系统，入侵者为了长期控制 Windows 个人计算机和服务器，除了安装木马程序外，还必须获取操作系统本身的账号和密码。所以，Windows 系统密码的获取与破解是攻防的必备基础，是后期继续渗透的前提和关键，掌握 Windows 操作系统密码 Hash 的获取和破解至关重要。

本章着重介绍 Windows 操作系统如何通过 GetHashes、gsecdump 等工具快速获取密码 Hash 值并破解其密码，同时对扫描 3389 口令、自动获取 3389 口令、安全设置操作系统密码、检查系统账号是否被克隆等内容进行了介绍。

本章主要内容

- 使用 GetHashes 获取 Windows 系统密码
- 使用 gsecdump 获取 Windows 系统密码
- 使用 Quarks PwDump 获取域控密码
- 使用 PwDump 获取系统账号和密码
- 使用 SAMInside 获取及破解 Windows 系统密码
- Windows Server 2003 域控服务器用户账号和密码的获取
- 使用 Ophcrack 破解系统 Hash 密码
- 使用 oclHashcat 破解 Windows 系统账号和密码
- 使用 L0phtCrack 破解 Windows 和 Linux 的密码
- 通过 hive 文件获取系统密码 Hash
- 使用 Fast RDP Brute 破解 3389 口令

- Windows 口令扫描攻击
- 使用 WinlogonHack 获取系统密码
- 检查计算机账号克隆情况
- 安全设置操作系统的密码

1.1 使用 GetHashes 获取 Windows 系统密码

对入侵者来说，获取 Windows 口令是整个攻击过程中至关重要的一环，拥有用户的口令将使内网渗透和守控更加容易。Windows 系统中的 Hash 密码值主要由 LM-hash 值和 NTLM-hash 值两部分构成，一旦入侵者获取了系统的 Hash 值，通过 LC5 及彩虹表等破解工具就可以很快获取系统的密码。

本节主要探讨如何使用 GetHashes 工具获取系统的 Hash 值，并对 Hash 值的生成原理等知识进行讲解，最后介绍了一些有关 Hash 破解方面的技巧。

1.1.1 Hash 的基础知识

本节介绍与 Hash 相关的基础知识。

1. Hash 的定义

Hash，一般翻译为“散列”，也有直接音译为“哈希”的，就是把任意长度的输入（又叫做预映射，Pre-Image）通过散列算法变换成固定长度的输出，该输出就是散列值。这种转换是一种压缩映射，也就是散列值的空间通常远小于输入的空间，不同的输入可能会散列成相同的输出，故不可能从散列值来唯一确定输入值。简单地说，Hash 就是一种将任意长度的消息压缩到某一固定长度的消息摘要函数。

2. Hash 的应用

Hash 主要用于信息安全领域的加密算法，它把一些不同长度的信息转化成杂乱的 128 位编码，这种编码叫做 Hash 值。可以说，Hash 就是找到数据内容和数据存放地址之间的映射关系。

3. Hash 算法在密码上的应用

MD5 和 SHA1 可以说是目前应用最广泛的 Hash 算法，它们都是以 MD4 为基础设计的，下面简单介绍一下。

- MD4（RFC 1320）是 MIT 的 Ronald L. Rivest 在 1990 年设计的，“MD”是“Message Digest”的缩写。MD4 在 32 位字长的处理器上通过高速软件实现，

它是基于32位操作数的位操作来实现的。

- MD5（RFC 1321）是Rivest于1991年对MD4的改进版本。它仍以512位分组来输入，其输出与MD4相同，是4个32位字的级联。MD5比MD4来得复杂，并且速度要慢一些，但MD5比MD4更安全，在抗分析和抗差分方面表现更好。
- SHA-1是由NIST NSA设计的，与DSA一起使用。它对长度小于264位的输入产生长度为160位的散列值，因此抗穷举（Brute-Force）性更好。SHA-1设计时基于和MD4相同的原理，并且模仿了该算法。

Hash算法在信息安全方面的应用主要体现在以下3个方面。

（1）文件校验

我们比较熟悉的校验算法有奇偶校验和CRC校验，这两种校验并没有抗数据篡改的能力，它们在一定程度上能检测并纠正数据传输中的信道误码，但不能防止对数据的恶意破坏。MD5 Hash算法的“数字指纹”特性，使它成为目前应用最广泛的一种文件完整性校验和（Checksum）算法，不少UNIX系统提供了计算MD5 Checksum的命令。

（2）数字签名

Hash算法也是现代密码体系的一个重要组成部分。由于非对称算法的运算速度较慢，所以在数字签名协议中，单向散列函数扮演了一个重要的角色。对Hash值（又称“数字摘要”）进行数字签名，在统计上可以认为与对文件本身进行数字签名是等效的。

（3）鉴权协议

鉴权协议又称挑战-认证模式，在传输信道可被侦听但不可被篡改的情况下，这是一种简单而安全的方法。

1.1.2 Windows的Hash密码值

下面我们讨论一下Windows的Hash密码值。

1. Windows系统的Hash密码格式

Windows系统的Hash密码格式如下。

```
用户名称:RID:LM-hash值:NT-hash值
```

Windows系统的Hash密码示例如下。

```
Administrator:500:C8825DB10F2590EAAAD3B435B51404EE:683020925C5D8569C23AA
724774CE6CC:::
```

- 用户名：Administrator
- RID：500
- LM-hash 值：C8825DB10F2590EAAAD3B435B51404EE
- NT-hash 值：683020925C5D8569C23AA724774CE6CC

2. Windows 下 LM-hash 值的生成原理

假设明文口令是“Welcome”，首先全部转换成大写，即“WELCOME”，再将该大写字符串转换成二进制串“57454C434F4D4500000000000000”。

技巧

可以将明文口令复制到 UltraEdit 编辑器中，使用二进制方式查看即可获取口令的二进制串。

如果明文口令经过大写变换后的二进制字符串不足 14 字节，则需要在其后添加“0x00”来补足 14 字节。

将转换后的二进制串切割成 2 组 7 字节的数据，分别经 str_to_key() 函数处理，得到 2 组 8 字节数据。

- 57454C434F4D45→56A25288347A348A
- 00000000000000→0000000000000000

说明

str_to_key() 函数的 C 语言描述如下。

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
/*
* 读取形如“AABBCCDDEEFF”的 16 进制数字串，由主调者进行形参的边界检查
*/
static void readhexstring ( const unsigned char *src, unsigned char *dst,
unsigned int len )
{
    unsigned int  i;
    unsigned char str[3];

    str[2] = '\0';
    for ( i = 0; i < len; i++ )
    {
        str[0] = src[ i * 2     ];
```