"An in-depth tour of what we use to get the job done."
—Dan Kaminsky

SECURITY POWER TOOLS

计算机安全超级工具集

Bryan Burns, Jennifer Stisa Granick, Steve Manzuik, Paul Guersch, Dave Killion, Nicolas Beauchesne, Eric Moret, Julien Sobrier, Michael Lynn, Eric Markham, Chris Iezzoni & Philippe Biondi 著

李展 贺民 周希 译

O'REILLY®

清华大学出版社

计算机安全超级工具集

Bryan Burns, Jennifer Stisa Granick, Steve Manzuik,
Paul Guersc[illegible] Killion, Nicolas Beauchesne,
Eric Moret, Julien S[illegible]n, Eric Markham,
[illegible]hilippe Biondi 著

李展 贺民 周希 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Sebastopol • Taipei • Tokyo

O'Reilly Media, Inc. 授权清华大学出版社出版

清华大学出版社

图书在版编目（CIP）数据

计算机安全超级工具集/（美）伯恩（Burns, B.）等著；李展等译. —北京：清华大学出版社，2009.6
书名原文：Security Power Tools
ISBN 978-7-302-19439-2

I. 计… II. ①伯… ②李… III. 电子计算机－安全技术 IV. TP309

中国版本图书馆 CIP 数据核字（2009）第 015989 号

责任编辑：龙啟铭
封面设计：Mike Kohnke，张　健
责任校对：徐俊伟
责任印制：孟凡玉
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**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
印 刷 者：清华大学印刷厂
装 订 者：三河市金元印装有限公司
经　　销：全国新华书店
开　　本：178×233　　**印　　张**：45　　**字　　数**：906 千字
版　　次：2009 年 6 月第 1 版　　**印　　次**：2009 年 6 月第 1 次印刷
印　　数：1～3000
定　　价：99.00 元（册）

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103　　产品编号：025877-01

O'Reilly Media, Inc. 介绍

为了满足读者对网络和软件技术知识的迫切需求，世界著名计算机图书出版机构O'Reilly Media, Inc. 授权清华大学出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly Media, Inc. 是世界上在 UNIX、X、Internet 和其他开放系统图书领域具有领导地位的出版公司，同时也是联机出版的先锋。

从最畅销的 *The Whole Internet User's Guide & Catalog*（被纽约公共图书馆评为20世纪最重要的50本书之一）到GNN（最早的Internet门户和商业网站），再到WebSite（第一个桌面PC的Web服务器软件），O'Reilly Media, Inc. 一直处于Internet发展的最前沿。

许多书店的反馈表明，O'Reilly Media, Inc. 是最稳定的计算机图书出版商 —— 每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly Media, Inc. 具有深厚的计算机专业背景，这使得 O'Reilly Media, Inc. 形成了一个非常不同于其他出版商的出版方针。O'Reilly Media, Inc. 所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly Media, Inc. 还有许多固定的作者群体 —— 他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly Media, Inc. 依靠他们及时地推出图书。因为 O'Reilly Media, Inc. 紧密地与计算机业界联系着，所以 O'Reilly Media, Inc. 知道市场上真正需要什么图书。

译者序

有人说人与动物的根本区别，就是会制造和使用工具。亚里士多德有这样一句名言，“给我一个支点，我就可以翘动地球”。理论上这是可行的。当然，仅仅有支点是不够的，还需要使用杠杆，杠杆就是工具，我们可以看到工具的重要作用。

其实，工具无处不在。我们吃饭，需要工具（筷子，碗等）；我们工作，需要工具（电脑，鼠标等）；我们出行，需要工具（自行车，公交车等），就是简单地钉几页纸，也需要钉书器或曲别针之类的小工具，画一条直线、画一个圆呢，会需要板尺和圆规……工具，可以说在我们的生活中随时随地为我们服务，提供帮助。当然，没有这些工具，我们也可以生活或工作，比如，画直线，画圆，徒手完全可以，但总不会有使用板尺画的线条那么笔直，也不会有使用圆规画的圆圈那么圆；出行走路也可以，但总不如坐车的速度快。

计算机软件工具，可以说浩如烟海。本书所选的工具，仅仅针对安全问题。这是因为，在使用电脑的过程中，安全问题已经成为人们不可忽视的重要问题。现在，随着Internet的流行，很少有不联网的孤岛一样的计算机，人们在从网络中共享信息、轻松聊天、互通邮件等受益的同时，也面临着许多风险。影响到计算机系统安全的不仅仅是简单的病毒，还有大量来自网络的攻击，也许在你不知不觉中，黑客和垃圾邮件传播者可能正在悄悄利用你的计算机，把它作为任人宰割的“肉鸡”，他们悄悄入侵，用恶意软件获取信息，包括邮件程序。一旦你上线，他们就可以上网记录，盗取信息，并控制你的邮箱发送垃圾邮件，使你成为僵尸网络中的一部分。而对于企业来说，网络安全则更为重要，因为它甚至有可能影响到企业的效益和生存。计算机安全的重要性再怎么强调也不过分。

本书讲解的辅助网络安全的工具，有免费软件，还有商用软件，它们都极为优秀。本书讲解的诸多网络安全工具都是作者精挑细选的，也许你正在烦恼苦思冥想的安全难题，使用本书介绍的一个看起来不起眼的小工具就可以迎刃而解了。这本书最主要的作用就是，书中介绍的工具可以帮助您提高效率，保护好计算机和网络，更出色地完成任务。

本书主要由李展、贺民、周希翻译，参加翻译的还有韦笑、王雷、李志云、李晓春、陈安华、孙宏、侯佳宜、许伟、戴文雅、于樊鹏、刘朋、王嘉佳、李腾、邓卫、邓凡平、陈磊、李建锋、刘延军、魏宇、赵远锋、樊旭平、唐玮、周京平、徐冬、冯哲、李绯、李强、赵东辉、宋雁、吴江华、孙燕、周刚、张乐华、高强、王红亮、周峰、

谢晖、李琳、刘明涛、孙向阳、李波、程云建、许晓哲、朱珂、李元园、曹锋、赵志鹏、冯佳、李健、林彩娥、孙蕾、杨金奎、张百涛、李展、张文波、赵楠、周文培、连祥宇、刘欣、李昊丞、黄虹、侯文茹、胡平等人。最后，祝广大读者从本书中挖掘出更多的宝藏。

封面介绍

本书封面上的图称为电锤。这种工具也称为锤钻，用于钻石头或水泥。它利用一个旋转的钻头，往石头上钻孔，快而且不费力。旋转速度低的时候，也可以用它来凿空和更精确的切割。

封面图由 Frank Deras 拍摄。

目录

序 1

创作者队伍 3

前言 7

第一部分 法律和道德

1 法律和道德问题 19

1.1 核心问题 20

1.2 计算机入侵法规：不允许“黑客入侵” 22

1.3 逆向工程 28

1.4 漏洞公布 35

1.5 今后要做什么 39

第二部分 检测工具

2 网络扫描 43

2.1 扫描器的工作方式 43

2.2 超级用户权限 45

2.3 三种网络扫描器 45
2.4 主机发现 46
2.5 端口扫描 48
2.6 指定自定义端口 50
2.7 指定扫描目标 51
2.8 不同的扫描种类 52
2.9 调整扫描速度 55
2.10 应用程序指纹识别 58
2.11 操作系统检测 59
2.12 保存 Nmap 输出 60
2.13 恢复 Nmap 扫描 61
2.14 检测规避 61
2.15 结论 63

3 漏洞扫描 64
3.1 Nessus 64
3.2 Nikto 79
3.3 WebInspect 82

4 局域网搜索 93
4.1 映射局域网 94
4.2 交换网中使用 ettercap 和 arpspoof 95
4.3 处理静态 ARP 表 98
4.4 从局域网获取信息 100
4.5 操作数据包数据 104

5 无线搜索 107
5.1 获得正确的驾驶攻击设备 107
5.2 802.11 网络基础 108
5.3 802.11 帧 109
5.4 无线网络发现工具的工作方式 110
5.5 Netstumbler 110
5.6 Kismet 一瞥 112
5.7 使用 Kismet 115

5.8 对 Kismet 网络列表分类 116
5.9 利用 Kismet 使用网络组 117
5.10 通过调查请求来利用 Kismet 寻找网络 117
5.11 利用 gpsd 支持 Kismet GPS 118
5.12 利用 Kismet 仔细观测流量 119
5.13 使用 Kismet 捕获数据包和破解流量 120
5.14 Wireshark 一瞥 122
5.15 使用 Wireshark 124
5.16 AirDefense Mobile 126
5.17 AirMagnet 分析器 129
5.18 其他驾驶攻击工具 132

6 自定义数据包生成 134
6.1 创建自定义数据包的原因 134
6.2 hping 136
6.3 Scapy 139
6.4 使用 Scapy 构建数据包示例 161
6.5 使用 Netfilter 进行数据包处理 179
6.6 参考资料 183

第三部分 渗透工具

7 Metasploit 187
7.1 Metasploit 界面 188
7.2 更新 Metasploit 193
7.3 选择漏洞 193
7.4 选择有效载荷 194
7.5 设定选项 198
7.6 运行漏洞 200
7.7 管理会话和工作 203
7.8 Meterpreter 205
7.9 安全设备规避 209
7.10 规避输出摘要 210

7.11 使用编码器和 NOP 的规避 211
7.12 结论 213

8 无线渗透 214
8.1 WEP 以及 WPA 加密 214
8.2 Aircrack 215
8.3 安装 Aircrack-ng 216
8.4 运行 Aircrack-ng 218
8.5 Airpwn 219
8.6 Airpwn 基本使用 220
8.7 Airpwn 配置文件 223
8.8 在 WEP 加密的网络上使用 Airpwn 224
8.9 使用 Airpwn 运行脚本 225
8.10 Karma 226
8.11 结论 228

9 探测框架应用程序 229
9.1 任务总览 229
9.2 Core Impact 概述 230
9.3 使用 Core Impact 搜索网络 233
9.4 Core Impact 探测搜索引擎 233
9.5 运行探测 235
9.6 运行宏 236
9.7 试探安装的代理 238
9.8 使代理在重新引导后仍存在 239
9.9 大范围探测 239
9.10 为 Core Impact 编写模块 240
9.11 Canvas 探测框架 242
9.12 使用 Canvas 进行探测移植 244
9.13 在命令行中使用 Canvas 245
9.14 深入挖掘 Canvas 246
9.15 带有 MOSDEF 的高级探测 246
9.16 为 Canvas 编写探测 247
9.17 备选探测工具 250

10 自定义探测程序 251
10.1 理解探测 252
10.2 分析 shell 代码 257
10.3 测试 shell 代码 260
10.4 创建 shell 代码 265
10.5 伪装 shell 代码 280
10.6 执行流劫持 283
10.7 参考书目 295

第四部分 控制工具

11 后门程序 299
11.1 选择后门程序 300
11.2 VNC 301
11.3 创建 VNC 后门程序且打包 302
11.4 连接以及移除 VNC 后门程序 307
11.5 Back Orifice 2000 309
11.6 配置 BO2k 服务器 310
11.7 配置 BO2k 客户端 314
11.8 向 BO2k 工作界面中添加新服务器 316
11.9 使用 BO2k 后门 317
11.10 BO2k 的强大工具 318
11.11 BO2k 通信的加密手段 328
11.12 隐藏 BO2k 协议 329
11.13 移除 BO2k 331
11.14 Unix 后门程序 332

12 Rootkit 335
12.1 Windows Rootkit：计算机黑客防卫者 335
12.2 Linux Rootkit：Adore-ng 337
12.3 Rootkit 探测技术 339
12.4 Windows Rootkit 检测器 342
12.5 Linux Rootkit 检测器 347

12.6 清理感染的系统 351
12.7 Rootkit 的特性 351

第五部分 防御工具

13 前摄防御：防火墙 355
13.1 防火墙初步 355
13.2 网络地址转换 358
13.3 使用 ipfw/natd 保护 BSD 系统安全 360
13.4 使用 netfilter /iptable 保护 GNU/Linux 系统 369
13.5 带有 Windows 防火墙 /Internet 连接共享 Windows 系统的安全措施 379
13.6 校验范围 384

14 主机加固 387
14.1 控制服务 388
14.2 关闭不需要的服务 389
14.3 访问限制 390
14.4 减小损害 394
14.5 Bastille Linux 399
14.6 SELinux 401
14.7 密码破译 406
14.8 chroot 409
14.9 操作系统的虚拟沙盒 410

15 通信安全保护 416
15.1 SSH-2 协议 417
15.2 SSH 的配置 419
15.3 SSH 认证 424
15.4 SSH 的不足 428
15.5 SSH 故障处理 435
15.6 使用 SSH 远程访问文件 438
15.7 SSH 高级用法 441
15.8 在 Windows 中使用 SSH 445

15.9 文件和电子邮件的签名和加密 450
15.10 GPG 451
15.11 创建 GPG 密钥 455
15.12 使用 GPG 加密和签名 461
15.13 PGP 和 GPG 的兼容性 463
15.14 使用 S/MIME 加密和签名 464
15.15 Stunnel 466
15.16 磁盘加密 474
15.17 使用 PGP 磁盘进行 Windows 文件系统加密 474
15.18 使用 LUKS 进行 Linux 文件系统加密 474
15.19 结论 476

16 电子邮件安全和反垃圾邮件 477
16.1 Norton 反病毒软件 478
16.2 ClamAV 项目 482
16.3 ClamWin 482
16.4 Freshclam 484
16.5 clamscan 487
16.6 clamd 和 clamdscan 488
16.7 ClamAV 病毒特征 494
16.8 Procmail 497
16.9 基本 Procmail 规则 499
16.10 高级 Procmail 规则 502
16.11 ClamAV 和 Procmail 503
16.12 无请求邮件 503
16.13 使用 Bayesian 过滤器过滤垃圾邮件 505
16.14 SpamAssassin 508
16.15 SpamAssassin 规则 511
16.16 SpamAssassin 插件 515
16.17 SpamAssass 和 Procmail 517
16.18 反钓鱼工具 519
16.19 结论 522

17 设备安全测试 523
17.1 使用 Tcpreply 重放数据 523
17.2 Traffic IQ Pro 532
17.3 ISIC 工具包 539
17.4 Protos 545

第六部分 监视工具

18 网络抓包 551
18.1 tcpdump 551
18.2 Ethereal/Wireshark 557
18.3 pcap 实用工具：tcpflow 和 Netdude 574
18.4 Python/Scapy 脚本修补校验 577
18.5 结论 580

19 网络监控 581
19.1 Snort 581
19.2 部署 Snort 591
19.3 蜜罐监控 592
19.4 综述 599

20 主机监控 602
20.1 使用文件完整性检查 602
20.2 文件完整性哈希 604
20.3 使用 rpmverify 进行 DIY 606
20.4 对比文件完整性检查工具 607
20.5 为 Samhain 和 Tripwire 准备环境 610
20.6 使用 Samhain 和 Tripwire 初始化数据库 615
20.7 使用 Samhain 和 Tripwire 防护基准存储 616
20.8 使用 Samhain 和 Tripwire 运行文件系统检查 618
20.9 使用 Samhain 和 Tripwire 管理文件更改和更新存储数据库 620
20.10 使用 Samhain 和 Tripwire 识别恶意行为 622
20.11 使用 Logwatch 监视日志 624

20.12 改进 Logwatch 的过滤器 625
20.13 使用 Prelude-IDS 在大型网络环境下的主机监控 626
20.14 结论 628

第七部分 发现工具

21 Forensic 工具 631
21.1 Netstat 632
21.2 Forensic ToolKit 635
21.3 Sysinternal 640

22 应用程序干扰 653
22.1 使用哪个干扰器 654
22.2 完成不同任务的不同类型干扰器 655
22.3 用 Spike 写干扰器 660
22.4 Spike API 661
22.5 文件干扰程序 665
22.6 干扰 Web 应用程序 667
22.7 配置 WebProxy 669
22.8 使用 Webnspect 自动干扰 670
22.9 下一代干扰器 671
22.10 干扰还是不干扰 672

23 二进制逆向工程 673
23.1 Interactive Disassembler 673
23.2 Sysinternals 695
23.3 OllyDbg 696
23.4 其他工具 699

序

十五年前，当我第一次接触信息安全时，它的概念与我们的理解完全不同。那时，其重点主要是网络访问列表、强密码以及主机的强化。分布式系统的概念刚刚开始出现，而且，基于用户的网络由哑终端或初级网络操作系统组成。家庭环境也不是面向网络的，当然无法和现在相提并论。人们只能在1200或2400波特的速率上扮演攻击者或牺牲者的角色。

攻击和防御工具也相当初级。一定程度上，最高级的安全工作就是——现在依然是病毒/防病毒。还记得1988年的DOS乒乓球病毒吗？当时的安全防护也十分初级，实质上仅局限于高端企业以及政府机构。

简单来说，安全是一种类似保护的方法，可通过隔离方式来实现。虽然还有局限性，但网络连接具有严格的访问控制。因此，网络并不被认为是攻击的首要传播途径。

现在来看，安全状况已经全然不同。这种变化起初是缓慢的，随着Internet的增长而不断迅速发展。毫无疑问，Internet的应用以及TCP/IP作为通用协议的使用，对越来越多的攻击传播起到了主要的催化剂作用。因而，就产生了对更多更强大防御机制的需求，同时相应产生了供给。就防病毒产业而言，这种猫鼠游戏过程既改进了攻击工具，也提高了防御工具的复杂性。Internet的普遍应用，也使其成为具有很多攻击目标的环境，而且，它还为攻击者提供了诸多可以发起攻击的地方。

在安全状况改变的同时，围绕安全这一主题展开的讨论也发生了变化。借用密码学领域的术语来讲，安全的实现主要是通过“隐匿”。我仍然记得，某些人士偏爱评论NT的防火墙邮件列表，原因就是它新奇和不为人所知，比开放源码的Unix更加安全。时间证明，虽然“隐匿安全”在某些领域内是有效的策略，但它在大多数信息安全相关领域并不起作用。

伴随着这项产业的成熟，我们亲眼目睹了相关概念的发展，变得越来越完整、可靠和公开。每家企业都在逐步提高安全意识，以及对安全事务的反应能力。微软曾经一度由于其安全状况而被世人所嘲笑，现在看，它已经是安全反应方面真正的先驱。如果考虑到他们支持的代码数量以及庞大的用户群，可想而知，很难找到任何一家软件供应商能为客户提供如此非凡的安全支持。