

网络与信息安全技术经典丛书

继“黑客大曝光”
之后的又一力作



HARDENING

Windows Systems 中文版

Bulletproof your systems before you are hacked!
为你的系统构筑坚固的安全堡垒

[美] Roberta Bragg 著

吴晓斌 程文俊 译

Mc
Graw
Hill

Osborne

Mc
Graw
Hill

清华大学出版社

网络与信息安全技术经典丛书

Hardening Windows Systems 中文版

[美] Roberta Bragg 著

吴晓斌 程文俊 译

清华大学出版社
北京

Roberta Bragg
Hardening Windows Systems
EISBN 0-07-225354-1
Copyright © 2004 by The McGraw-Hill Companies.

Original language published by the McGraw-Hill Companies, Inc. All Rights reserved. No part of this publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

Simplified Chinese translation edition is published and distributed exclusively by Tsinghua University Press under the authorization by McGraw-Hill Education (Asia) Co., within the territory of the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan. Unauthorized export of this edition is a violation of the Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书中文简体字翻译版由美国麦格劳-希尔教育出版(亚洲)公司授权清华大学出版社在中华人民共和国境内(不包括中国香港、澳门特别行政区和中国台湾)独家出版发行。未经许可之出口,视为违反著作权法,将受法律之制裁。未经出版者预先书面许可,不得以任何方式复制或抄袭本书的任何部分。

版权所有,翻印必究。举报电话:010-62782989 13501256678 13801310933

本书封面贴有 McGraw-Hill 公司防伪标签,无标签者不得销售。

北京市版权局著作权合同登记号 图字 01-2006-0350 号

图书在版编目(CIP)数据

Hardening Windows Systems 中文版/(美)布拉格(Bragg, R.)编著;
吴晓斌,程文俊译. —北京:清华大学出版社,2006.5
书名原文:Hardening Windows Systems
ISBN 7-302-13040-X

I. H... II. ①布... ②吴...③程... III. 窗口软件, Windows
IV. TP316.7

中国版本图书馆 CIP 数据核字(2006)第 049556 号

出版者:清华大学出版社

<http://www.tup.com.cn>

社总机:010-62770175

地址:北京清华大学学研大厦

邮编:100084

客户服务:010-82896445

组稿编辑:夏非彼

文稿编辑:何武

封面设计:林陶

版式设计:科海

印刷者:北京市耀华印刷有限公司

发行者:新华书店总店北京发行所

开本:185×230 印张:29 字数:633千字

版次:2006年6月第1版 2006年6月第1次印刷

书号:ISBN 7-302-13040-X/TP·8277

印数:0 001~3 000

定价:53.00元

本书如存在文字不清、漏印以及缺页、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) 82896445

内 容 提 要

“Hardening”系列是美国 McGraw-Hill 公司新近推出的又一套信息安全系列丛书，与久负盛名的“黑客大曝光”系列携手，为信息安全界奉献了一道饕餮大餐。

本书是“Hardening”系列成员之一，由安全界著名传道士 Roberta Bragg 执笔，通过四段式系统强化教学法，从技术和管理制度两方面，详细介绍 Windows 系统的安全防护工作，对系统管理员容易疏忽或犯错的细节进行深入发掘，旨在帮助读者把 Windows 系统建设成坚固的信息安全堡垒。

全书共分 4 大部分 14 章，第 1 部分给出降低系统威胁的 10 项关键措施，是系统阻止入侵的必要手段；第 2 部分是本书的重中之重，自顶向下系统讲述强化 Windows 系统的各项具体方法和措施；第 3 部分告诫人们：一劳不能永逸，需要利用各种监控技术持续监控系统，教会读者创建业务连续性计划、制定安全策略以及灾难恢复策略等；第 4 部分对信息安全工作的湿件方面进行全方位讨论，同类书中少见。

本书操作平台覆盖 Windows 95/98/NT 4.0/2000/XP 以及 Windows Server 2003，是 IT 专业人士的福音。

作者简介

Roberta Bragg, CISSP, M.C.S.E.: Security, Security+, 在 IT 界从业 25 年, 从大型主机到移动系统, 从穿孔卡片到 .NET, 从拨号上网到 Internet, 她一直是活跃人物并创造了很多神话。当前承担的项目包括高级的、短期的有关 Windows 安全方面的咨询业务, 长期担任 MCP Magazine Security Advisor 杂志的安全领域专栏作者, 还是 TechTarget Win2000 Security Expert Q & A 的特邀顾问。Roberta Bragg 是 McGraw-Hill/Osborne 公司出版的 Hardening 系列图书的策划人, 本套图书旨在帮助读者在遭受黑客攻击之前系统地加固自己的网络。

序 言

最近三年，系统安全问题已经从发生事故后 IT 部门的事后反思，变成了决策时首先需要考虑的问题，其重要性日益凸显。系统安全越来越重要的后果是，不仅需要大量合格的安全专家，而且对几乎所有的 IT 管理员来说，是否懂得系统安全已成为一项非常重要的工作需求。但是对大多数的 IT 管理员来说，他们日常本身已没有足够的时间来完成手头现有的工作，更不必说花费时间来搜集大量的文献、书籍和网站等信息来加强他们的 Windows 操作系统，特别是如果公司的网络使用 Windows 不同版本的系统，那将更麻烦。如果你遇到了上述问题，那么这本书将是你的最好选择。此书将给你全面细致的系统安全解决方案。

在读此书的初稿时，Roberta 女士在加强 Windows NT 4.0, Windows XP, Windows 2000 和 Windows Server 2003 等系统安全方面出色的工作给我留下了深刻的印象。市面上大多数系统安全书籍只讲述一至二个 Windows 操作系统，很少像本书一样涉及全部 Windows 系统，特别是作为一点小奖励，Roberta 女士更是讲了一些 Windows 95 和 Windows 98 系统安全的小技巧。再加上她随和、轻松的写作风格，这本书将是一本独一无二的系统安全宝典。（我认识 Roberta 女士已很多年，在读此书时，字里行间仿佛都能听到她的声音。）

本书另一个突出的优点就是其方案的可操作性很强，虽然计算机安全是计算机本身的事情，但最大的安全漏洞往往是人。好消息是，一旦人们得到良好的训练，他们就是你可配置的最好安全措施；坏消息是，很显然，你无法按组策略来配置他们。本书详细阐述了计算机、用户、管理员和 IT 管理人员之间相互关联的能够引发网络攻击的一些重要领域，并介绍了一些除安全配置之外的技术措施。

我可以很有信心地说，通过阅读此书，你将能熟练出色地加强公司客户端和服务器的 Windows 操作系统的安全。

Ben Smith
Security Strategist
Microsoft Corporation

“一个优秀的系统安全领路人——我自认无法比她写得更好。一本全面、通俗易懂的 Windows 系统安全参考书。每个系统管理员必读的宝典。”

Eric Schultze

首席安全架构师，Shavlik Technologies

微软高信度计算小组前成员

前 言

生活如大多数人想的一样充满各种危险因素，如果我们想幸免于难，就必须做好信息系统的安全防范工作，必须学会如何更好地防护信息系统，以及极力阻止那些粗枝大叶，甚至用心险恶，或者口无遮拦的人可能对系统造成的任何破坏。

信息防护是一项繁重到几乎不可思议的工作。但在我们遇到大问题等待安全专家救驾时，还是可以采取一些适当的弥补措施。问题的关键是，我们不应该等待、犹豫——而是应该立马采取行动。在我们与他人合作或独自工作时，应努力营造一种安全文化，加强所有牵涉到的网络组件的安全，建造一个更安全的系统，并把此理念灌输给每个员工。如果你从事 IT 行业，那更应有此观念！本书所属的“Hardening”系列丛书，能给你提供一些帮助。此系列丛书中的每本书分别涉及信息系统的一个部分，并为每个部分提供了相应的系统强化措施。

本书为强化 Windows 系统的一些必要步骤罗列了一个主要的目录，适用于 Windows 98, Windows 95, Windows NT 4.0, Windows 2000, Windows XP 以及 Windows Server 2003 系统。本书不想成为信息安全的一个全面向导，也不可能包含理解和实践 Windows 安全所必需的全部信息。但本书叙述详尽而且简单易懂，每一强化步骤都附有一步步的详细说明。对部分读者，本书为您提供了一个开始强化信息系统安全的平台；对另一部分读者，本书所列举的措施可用于判断您目前采取的措施是否正确；对其他一些读者，本书可为您的 Windows 系统安全知识打下坚实的基础。

请您阅读、吸收，然后使用书中的知识。如果您觉得本书好，请推荐给您的朋友。如果您觉得本书不尽人意，请告诉我们。但最重要的，请强化您的 Windows 系统。

致 谢

感谢 Athena Honore 一直给我善意的提醒；感谢组稿编辑 Tracy Dunkelberger，一位出色的组稿编辑，也是我的拳击陪练；感谢文稿编辑 Bob Campbell 给本书润色不少；感谢计划编辑 Emily Rader 统筹一切事情；感谢技术编辑 Rodney R.Fournier；以及其他一些我不知名的对本书出版做出贡献的人们。

我还将感谢所有使整个世界的信息系统更加安全的读者朋友们，你们已经做了大量工作。你们将一直是我灵感和其他悲伤的来源。

目 录

第 1 部分 马上行动

第 1 章 立即行动	3
1.1 强化密码策略	5
1.1.1 创建逻辑策略	6
1.1.2 改变本地账户策略	7
1.1.3 修改个人账户策略	7
1.2 锁定远程管理	9
1.3 锁定管理工作站	10
1.4 物理保护所有系统	11
1.5 保密	11
1.6 禁用 EFS	12
1.7 禁用不满足严格安全策略要求的无线网络	12
1.8 禁止无保护措施的本机和台式机连接局域网	13
1.9 使用 Runas 或 Su	13
1.10 禁用红外文件传输	14

第 2 部分 从顶端做起：系统地强化安全

第 2 章 强化认证——证明来宾身份	17
2.1 什么是认证	18
2.1.1 何时需要认证	18
2.1.2 在 Windows 安全框架内何处适合认证	19
2.2 认证的证书 (credentials) 选择	20
2.3 强化用户登录	21
2.3.1 登录类型	22

2.3.2 强化账户	23
2.3.3 强化账户策略	24
2.3.4 强化湿件	36
2.3.5 禁止自动登录	38
2.3.6 限制匿名访问	39
2.3.7 保护 Windows 2000 系统的密码安全	40
2.4 强化网络认证	41
2.4.1 LM, NTLM, NTLMv2	41
2.4.2 Kerberos 协议	44
2.4.3 远程访问认证协议	45
2.4.4 Web 服务器认证选择	47
2.4.5 加强无线认证	48
2.5 强化计算机和服务的认证过程	48
2.5.1 为服务账号制定强密码以及不允许用户使用服务账号登录	49
2.5.2 使用本地服务账号并不允许通过网络访问服务账号	50
2.5.3 使用服务账号的低特权账号	50
2.5.4 强化计算机账户	50
第 3 章 强化物理网络基础设施	51
3.1 网络分段	52
3.1.1 示例	52
3.1.2 决定合适网络分段的最好方法	55
3.2 在分段边界安装防护性措施和检测性措施	57
3.2.1 防范性的控制措施	57
3.2.2 检测性的控制措施	64
3.2.3 边界控制的最好措施	65
3.3 保护重要通信	76
3.3.1 保护活动目录和其他域之间的通信	76
3.3.2 Web 通信保护	86
3.3.3 E-Mail 保护	86
3.4 保护重要服务器	86
3.4.1 保护域控制器	86
3.4.2 保护基础设施服务器	89

3.5 保护网络基础设施	89
3.6 保护对客户端系统的访问	90
3.6.1 使用常驻计算机的防火墙	90
3.6.2 客户端物理安全选项	91
第 4 章 强化逻辑网络基础设施	93
4.1 工作组计算机安全基础	94
4.1.1 工作组基本要点	95
4.1.2 工作组用户账号	95
4.1.3 工作组网络资源	95
4.1.4 强化工作组	97
4.2 Windows NT 4.0 类型的域的安全基础	99
4.2.1 中央管理	100
4.2.2 安全边界	100
4.2.3 NT 4.0 类型的信任	101
4.2.4 强化 Windows NT 4.0 域	103
4.3 活动目录林安全基础	104
4.3.1 中央集权管理的优点	105
4.3.2 自治和隔离：域不是一个安全边界	107
4.3.3 建立基于安全需要的域	108
4.3.4 建立基于安全和管理需要的组织单元	108
4.3.5 将域控制器和全局目录服务器只放在需要的地方	109
4.3.6 配置远程 Windows Server 2003 域控制器以使用通用组高速缓存	109
4.3.7 创建最小数目的异常域信任	110
4.3.8 提升域和林功能级别到 Windows Server 2003	113
4.3.9 使用选择性认证	116
4.3.10 如何建立一个外部信任 (External Trust)	118
4.4 强化逻辑网络基础设施的备忘录	122
第 5 章 强化网络基础设施角色	124
5.1 开发安全基线	126
5.2 限制用户权限	127
5.2.1 用户权限基线的修改	127

5.2.2 使用本地安全策略修改用户权限.....	129
5.2.3 使用 NT 4.0 用户管理器修改用户权限.....	129
5.3 禁用可选择的子系统	130
5.4 禁用或删除不必要的服务	131
5.5 应用混合安全配置	138
5.5.1 不显示上次登录用户名.....	139
5.5.2 添加登录提示	139
5.6 开发增量安全步骤 (Incremental Security Steps)	140
5.6.1 强化基础设施组 (Infrastructure Group)	140
5.6.2 强化 DHCP.....	140
5.6.3 强化 DNS	144
5.6.4 强化 WINS.....	152
5.7 选择安全部署的方法和模型	153
5.7.1 用工具在 Windows NT 4.0 系统进行常规安全设置.....	154
5.7.2 用安全模板定义安全设置.....	157
5.7.3 使用安全配置和分析或安全管理器.....	162
5.7.4 使用 Secedit.....	163
第 6 章 保护 Windows 目录信息及其操作.....	164
6.1 保护 DNS.....	166
6.2 将 AD 数据库和 SYSVOL 放在独立的磁盘上	167
6.3 物理保护域控制器	168
6.4 监视和保护活动目录状态	170
6.4.1 监视 DNS	170
6.4.2 监视复制	177
6.4.3 监视组策略操作	184
6.4.4 强化域以及域控制器安全策略.....	189
6.4.5 保护活动目录通信	193
6.4.6 管理“管理权限”(Administrative Authority)	194
6.5 保护活动目录数据——理解活动目录对象权限.....	195
第 7 章 强化管理权限和操作.....	196
7.1 委托和控制管理权限	197

7.1.1 定义用户角色	198
7.1.2 定义技术控制	209
7.2 定义安全管理措施	217
7.2.1 非常高风险管理	217
7.2.2 高风险数据中心管理	226
7.2.3 高风险非数据中心管理	229
7.2.4 中等风险管理	229
7.2.5 低风险管理	232
第 8 章 按角色分别强化服务器和客户端计算机	233
8.1 基于角色的强化过程	234
8.2 决定计算机角色	235
8.2.1 顶级计算机角色	236
8.2.2 二级或三级计算机角色	236
8.3 设计基于角色的强化基础设施	237
8.3.1 用脚本自动使用多模板	237
8.3.2 使用活动目录体系和组策略方法	239
8.3.3 使用 Windows NT 4.0 系统策略	243
8.4 改编安全模板	250
8.4.1 检查及修改基线模板	251
8.4.2 检查以及修改基于角色的模板	254
8.5 用组策略执行强化计划	255
8.5.1 创建一个撤销计划 (Back-out Plan)	256
8.5.2 将模板导入合适的 GPO	256
第 9 章 强化应用程序访问和使用	260
9.1 通过管理模板限制访问	261
9.1.1 强化操作系统配置	263
9.1.2 强化用户设置	268
9.1.3 使用其他.adm 文件	272
9.1.4 强化应用程序	273
9.2 通过软件限制策略限制访问	283
9.2.1 安全等级设置为 Disallowed	283

9.2.2 设置策略选项	284
9.2.3 编写规则来允许和限制软件	287
9.3 开发与实施台式机与用户角色	289
9.4 使用组策略管理控制台复制 GPO	291
第 10 章 强化数据访问	292
10.1 使用 NTFS 文件系统	293
10.2 使用 DACL 保护数据	294
10.2.1 使用继承管理权限	295
10.2.2 基于用户角色分配权限	297
10.2.3 维护合适权限	301
10.2.4 保护文件系统和数据	301
10.2.5 强化文件系统共享	305
10.2.6 保护打印机	309
10.2.7 保护注册表项	310
10.2.8 保护目录对象	312
10.2.9 保护服务	313
10.3 使用 EFS 保护数据	314
10.3.1 禁用 EFS 除非可被安全地使用	314
10.3.2 强化 EFS 规则	317
第 11 章 强化通信	322
11.1 保护 LAN 信息通信	323
11.1.1 为 NTLM 使用 SMB 消息签名和会话安全	323
11.1.2 使用 IPSec 策略	325
11.2 保护 WAN 信息通信	333
11.2.1 强化远程访问服务器	333
11.2.2 强化 NT 4.0 远程访问服务器配置	336
11.2.3 强化 Windows Server 2000 和 Windows Server 2003 RRAS 配置	338
11.2.4 使用 L2TP/IPSec VPN	342
11.2.5 使用远程访问策略	343
11.2.6 强化远程访问客户端	345
11.2.7 使用 IAS 集中认证、账户和授权	345

11.2.8 保护无线访问.....	346
11.3 用 SSL 保护 Web 通信	351
第 12 章 使用 PKI 强化 Windows 及强化 PKI 自身	352
12.1 使用 PKI 强化 Windows.....	353
12.1.1 使用 PKI 强化认证	353
12.1.2 用证书保护数据	359
12.2 强化 PKI	360
12.2.1 强化证书授权计算机.....	360
12.2.2 实施 CA 分级结构	360
12.2.3 保护根 CA.....	360
12.2.4 使用中间 CA 增加可靠性	366
12.2.5 在多个发行 CA 之间划分证书功能	368
12.2.6 为从属 CA 提供物理保护	368
12.2.7 要求证书批准	368
12.2.8 限制证书颁发	370
12.2.9 建立角色分离	372
12.2.10 强制角色分离	373
12.2.11 配置自动登记.....	374
12.2.12 培训用户证书请求程序.....	376
12.2.13 强化 PKI 策略、程序和规则	377

第 3 部分 一劳不能永逸

第 13 章 强化安全周期	381
13.1 创建业务连续性计划	382
13.1.1 确定计划范围	383
13.1.2 进行业务影响评估	383
13.1.3 进行风险分析	384
13.1.4 制定计划	385
13.1.5 测试	386
13.1.6 计划实施	386

13.1.7 计划维护	386
13.2 制定安全策略	386
13.3 强化操作系统安装	386
13.3.1 准备默认安全模板	387
13.3.2 使用 Slipstreaming	387
13.3.3 安装过程中用 RIS 添加服务包	387
13.3.4 安装过程中安装 Hotfix 补丁	388
13.4 强化操作系统、应用程序和数据保护	390
13.5 用正规的变更管理程序管理变更	391
13.5.1 升级、人员变动、变更和新的安装	392
13.5.2 安全配置更改	392
13.5.3 补丁	392
13.6 准备灾难恢复	403
13.6.1 使用容错配置	403
13.6.2 计划备份以及执行备份	404
13.6.3 计划并进行特殊备份操作	407
13.6.4 实践恢复操作	408
13.7 监控与审计	410
13.7.1 配置系统审计	411
13.7.2 配置审计日志	414
13.7.3 保存审计日志文件	415
13.7.4 使用安全事件进行入侵检测与辩论分析	416
13.7.5 审计安全配置	418
13.7.6 审计补丁状态	420

第 4 部分 如何成功地强化 Windows 系统的安全性

第 14 章 强化湿件 (Wetware)	425
14.1 诊断与改善安全策略	426
14.1.1 决定目前信息系统安全策略	427
14.1.2 评价策略	427
14.1.3 参与安全策略的构建与维护	428