科爱传播
KEAI COMMUNICATIONS

Perfect Passwords
Selection, Protection, Authentication

菜鸟也能防黑客之完美口令

Mark Burnett Dave Kleiman 著
陈 萍 季玉萍 周 虚 刘 琳 罗守山 译

● 11个标准检查你口令的安全性 ● 20项准则帮助你创建完美口令 ● 500个最差口令时刻提醒你不要成为『肉鸡』 ● 1000000个口令的研究分析结果教你如何构建强力又好记的口令

科学出版社
www.sciencep.com
ELSEVIER

Perfect Passwords

Selection, Protection, Authentication

菜鸟也能防黑客

完美口令

Mark Burnett
Dave Kleiman 著

陈萍 季玉萍 周虚 刘琳 罗守山 译

科学出版社

北京

图字：01-2009-0361 号

图书在版编目（CIP）数据

完美口令：菜鸟也能防黑客/（美）伯内特（Burnett, M.）等著；陈萍等译. —北京：科学出版社，2009

书名原文：Perfect Passwords: Selection, Protection, Authentication

ISBN 978-7-03-024897-8

Ⅰ.完… Ⅱ.①伯… ②陈… Ⅲ.电子计算机–密码术 Ⅳ.TP304.7

中国版本图书馆 CIP 数据核字（2009）第 107878 号

责任编辑：田慎鹏 霍志国 田 伟／责任校对：宋玲玲
责任印制：钱玉芬／封面设计：耕者设计工作室

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

双源印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2009 年 7 月第 一 版 开本：B5（720×1000）
2009 年 7 月第一次印刷 印张：12 3/4
印数：1—4 000 字数：252 000

定价：29.80 元

（如有印装质量问题，我社负责调换〈明辉〉）

作 者 简 介

Mark Burnett 是网络安全方面的顾问，同时他也是一位作家，并在基于 Microsoft Windows 的服务器与网络方面做过深入的研究。他在封锁 Windows 服务和确保 Windows 系统安全方面积累了十余年的经验。Mark 是 *Microsoft Log Parser Toolkit*（Syngress 出版，ISBN: 1-932266-52-6）一书的合作作者与技术编辑，是 *Hacking the Code:ASP.NET Web Application Security*（Syngress 出版，ISBN: 1-932266-65-8）一书的作者，是 *Maximum Windows 2000 Security*（SAMS 出版，ISBN: 0-672319-65-9）一书的合作作者，是 *Stealing the Network: How to Own the Box*（Syngress 出版，ISBN: 1-931836-87-6）一书的合作作者。他为 Dr.Tom Shinder 写的 *ISA Server and Beyond: Real World Security Solutions for Microsoft Enterprise Networks*（Syngress 出版，ISBN: 1-931836-66-3）一书提供了很多素材，为 *Special Ops: Host and Network Security for Microsoft, UNIX, and Oracle*（Syngress 出版，ISBN: 1-931836-69-8）一书提供了素材并作为技术编辑。Mark 在一些信息安全会议上做过发言，在一些杂志上发表过数十篇论文，这些杂志包括 *Windows IT Pro Magazine*, *Redmond Magazine*, *Windows Web Solutions*, *Security Administrator*, *Security Focus.com*, *TheRegister.co.uk* 和 *WindowsSecrets.com* 等。由于 Mark 在 Windows 社区与 Windows 服务器方面的工作，Microsoft 公司曾经两次授予他最有价值专家（Most Valued Professional, MVP）称号。

技术编辑

Dave Kleiman（CAS, CCE, CIFI, CISM, CISSP, ISSAP, ISSMP, MCSE）从 1990 年起就开始在信息安全部门工作。目前他拥有 SecurityBreachResponse.com 网站，同时也是 Securit-e-Doc 有限公司的首席信息安全官。在就任这个位置之前，他已经是 Intelliswitch 公司的技术运营副总经理。在该公司，他管理一个国际电信与互联网服务供应商网络。Dave 是公认的网络安全方面的专家。作为在佛罗里达通过认证的执法人员，他擅长于计算机取证调查、事件反应、入侵分析、安全分析和保护网络基础安全设施。他写了数部有关网络专业使用的微软技术的说明书。他开发了一个 Windows 操作系统系统锁定工具—— S-Lock（www.s-doc.com/products/slok.asp），该工具在功能上超越了 NSA、NIST 和微软公共标准指南。Dave 与其他人共同编写了 *Microsoft Log Parser Toolkit* 一书（ISBN 1-932266-52-6）。他经常在网络安全会议上发表演讲，是网络安全相关的时事通讯、Web 网站和互联网论坛的固定投稿人。Dave 是很多学术组织的成员，包括国际打击恐怖主义和安全专业人员国际协会（International Association of Counter Terrorism and Security Professionals, IACSP）、国际计算机取证协会（International Society of Forensic Computer Examiners, ISFCE）、信息系统审计与控制协会（Information Systems Audit and Control Association, ISACA）、高科技犯罪调查协会（High Technology Crime Investigation Association, HTCIA）、网络和系统专业人员协会（Network and Systems Professionals Association, NaSPA ），检查认证舞弊协会（Association of Certified Fraud Examiners, ACFE）、反恐怖主义鉴定委员会（Anti Terrorism Accreditation Board, ATAB）等。他也是 FBI 的安全专家和部门主管，也是国际信息系统鉴定组织（International Information Systems Forensics Association, IISFA）的教育主管。

技术审阅

Ryan Russell 已经在 IT 领域工作了 10 几年，多年来一直专注于信息安全研究。他是 *Hack Proofing Your Network, Second Edition* 一书的第一作者（Syngress, ISBN: 10928994-70-9），还是 *Stealing the Network: How to Own the Box*（Syngress, ISBN: 1-931836-87-6）一书的作者和技术编辑，也是 Stealing the Network 系列和 Hack Proofing 系列从书的技术编辑。他也是 *Snort 2.0 Intrusion Detection* 一书的技术顾问（Syngress, ISBN: 1-931836-74-4）。Ryan 建立了 vuln-dev 邮件列表，并且以 Blue Boar 的网名管理该列表三年。

目　录

Chapter 1

第1章
口令：基础及其他

下了马，他将马拴在一棵树上，然后向入口走去。他不会忘记那句话，他不断重复着："芝麻，开门哪"。于是，就像往常一样，门开了。他走了进去，看到那些金银宝藏还原封不动地在那儿放着。

——《天方夜谭：四十大盗》

引言

十年前，我拥有了第一份工作：软件开发员，也许从那时起我开始迷恋上了网络安全。时断时续，我编写代码也已经许多年了，但是，这是第一次有人聘请我做软件开发。我是一个公司雇员，我得整天写代码。我有一个网络账号，每天早上都会用它登录。几乎像公司的每个人一样，我用了很简单的口令，每隔三个月就会更换一次。当然，更换后的口令也一样简单。

长久以来，我对各个方面的安全都很感兴趣，但当时的所能获得的信息太少了。那个时候，还没有 Google 等搜索网站，你只能通过无止尽地点击一个又一个网站的链接来找到有用的信息。最后获取的信息往往是过时的、不可靠的，且局限于文本信息。所以结果我总是不满意。

尽管如此，我还是利用所有的空余时间去研究我所能找到的一切信息，打印了大量的资料，在一遍又一遍地研究后，我逐渐找到了些感觉。尽管我只是一个初学者，但仍旧学到了一些技巧，成为一个办公室黑客。

不久后的一个早上，我的一个朋友（也是某公司负责人之一）拉我到他的办公室，告诉我公司面临着一个困境，而且需要我的帮助。那天上午早些时候，公司的高级网络管理员与副总裁有过一次激烈的争执。在争吵过程中，网络管理员把他的钥匙甩在桌上，收拾好办公桌，就离开了公司。现在，公司的管理层要我进入所有的系统并恢复系统管理员的口令，因为副总裁实在不愿意打电话给那管理员索要口令。我知道面对这样的任务我没有经验，但我还是经不起挑战带来的诱惑。我告诉他，我会做到的。

但是当我坐下，冷静下来后，就意识到这项任务对我来说是多么的艰巨。我确实掌握了一些技巧，但我竟然妄想自己能完成这项任务，这真的很荒谬。我想，也许我应该向我的朋友坦承我没有他想的那么厉害。是我

想得太多，还是虚荣心在作怪？就算这事听起来并不合乎逻辑，但是我想，这也该是展现自己的时候了。

那天，如果我没有发现这样一个重要结论，我应该已经失败了。这个重要的结论就是：黑客们过人的技巧并不是他们成功的主要原因，我们每一个人在安全方面的疏忽大意才让黑客的破解行为变得如此轻松。我发现没有人使用强口令，而且，我们总是重复地使用那么几个相同的口令。每当涉及到口令的时候，我们似乎都变得没那么聪明了。

我先破解了管理员 Microsoft Access 中的口令，然后又破了他的电子邮箱口令。接下来，我又破了 Windows NT 的管理员口令。随着口令被一个一个的破解——superman12、superman23、superman95、Wonderwoman，他的安全防线彻底崩溃。

其实那天我并没有做什么特别的事情，只是发现了人们在网络安全中的一个致命弱点，那就是：人们使用的口令具有可怕的可预测性。那天深夜，我把口令清单用 e-mail 发给朋友。回到了家之后，我还一直沉浸在胜利的喜悦中。

第二天早上，我碰巧和公司总裁和副总裁同时到达办公楼，他们俩都转过身来，就好像事先已经排练好的一样，打开前门并向我鞠躬。我一开始感觉有点迷糊，但马上意识到他们已经知道我破了口令。我一边走进门一边为得到了公司高层的赏识而高兴。我喜欢像这样引起别人的注意，也是从那一刻起，我几乎疯狂地迷恋上了安全、口令以及人们的行为特征。

我们的口令

口令，不管以何种形式，长期以来一直与安全联系在一起。我们通常在文学作品上看到这样的描述：用口令打开一扇门，用口令通过一个防御，或使用口令来辨认敌我。这些模糊的字词或短语就是辨别间谍的魔咒。

口令也是现代生活中必不可少的一部分。我们使用它来检查电子邮件和语音信箱；我们利用它从 ATM 机上提款或是登陆到网上银行；我们利用它来进行金融交易或是网上购物；我们使用它来限制无线网络的访问，为我们的私人数据加密。当你定购比萨、购买鲜花、租 DVD 或是洗车时都需要口令。我们的世界充满了秘密。

描述口令的方式有很多，如 PIN、通行码，还有其他的描述。有了口令

这个秘密武器，我们才能获取生活中被保护的那部分信息。

口令不仅仅是一把钥匙，它有很多用途。它们可以通过某台机器对我们进行身份验证，当然这是只有我们自己知道的秘密；它们可以保护我们的隐私，确保一些敏感信息的安全；它们还是不容质疑的证据，使我们无法否认曾经使用口令进行过交易的事实。用户名可以识别身份，而口令用来验证我们的身份。

但是口令也有一些缺陷：在任何个时候都不只是一个人可以知道这个秘密。它不同于使用身体的某一部分的生物密钥，一次只有一个人可以拥有，所以你不能保证别人不会以某种方式获得你的口令，这些可能都是在你不知道的时候发生的。此外，恶意地把口令透露给别人，长期以来也是一个隐患。口令失窃是经常发生的事件，而且，在日常生活中也确实时常发生。你唯一可以采取的保护措施就是使用一个强有力的口令，小心地保护它，并且经常更换它。

口令的另一个缺陷跟人的行为有关。人的本性就是不会去认真对待那些没有察觉到的隐患。我们不会思考为什么会有人想获取我们电子邮箱或是上网账号。我们理所当然地认为自己选用的口令是安全的。

就在那一天，在上班的时候，当我从公司总裁和副总裁身旁走过之后，我走进门口，穿过大厅，坐在办公桌前。当我用我那简单的口令登录我网络账户时，突然，我被自己的这个疏忽震撼了。我意识到自己系统的安全性就跟前天被我破解的那个系统一样脆弱。就凭我最近使用的两个口令，别人很容易猜到我的当前口令以及将要使用的一个个口令。至少有一个同事已经知道我的口令，因为那天我生病了，我告诉了他口令以便他能访问我的文件。就在那一天，我就决定要改变我设口令这种草率的态度。

人类愚蠢的行为

几年前，我看了自称为精神病的 Kreskin 的一场表演，那是一场令人惊叹的表演。我一直仔细观察他不断地预测和操纵观众行为的过程。在表演过程中，他解释道：他并没有任何神奇的力量，只是对人的行为有一种特别的理解。

他不断地猜测着观众们挑选的秘密，并且都是跟很多观众个人生活中的事实联系在一起的那些秘密。例如他能够猜测出一些观众的社会保险号

码或是生日。能够做到猜测别人秘密的有很多人，如心理分析师、算命师、巫师、魔术师，以及其他类似的人，他们往往是依赖于人们行为的可预测性，获得猜测的成功。毫无疑问，这显示了人们只是不断地重复着自己的行为而已。

如果你让人说一个蔬菜的名字，98%的人会告诉你胡萝卜。如果让他们从 50 到 100 之间任意挑一个数，并要求这个数的两个数字是不同的，人们通常会选择 68。如果是挑一张牌，通常的选择就是方块 9、黑桃 A、红桃 Q 或者梅花 6。

你甚至可能发现自己在预测别人的行为或是其他事物的行为方面有着一些特殊技能，例如去推测一部电影的结局。值得注意的是，就像我们很难避免这种可预测性一样，我们能够发现他人的可预测性。

看一看表 1.1 中列出的随机口令，花几分钟的时间研究一下，你会发现其中出现了一些简单的可以预测的形式。

表 1.1　随机口令

bmw66	fuzzy1	trisha
Jessica1	Steven	123456
sa1856	Alexis	gregory2
843520	xmen94	brutus1
0214866	link11	lakers7
m9153p	1nani1	lamacod1
cyril87	Bubba1	pariz2
7082382	856899	letmein
100265	grady6	tiger69
jimmyd2	mpick1	cats999
wes333	mjordan2	supra1
053092	sti2000	bearcub
4Obelix	usa123	wargame6
6Bueler	Lieve27	dan1028
Franc1	3089172	13crow
Nicole3	Roswell	ncc1701
elin97	67bird	jun0214
toyota4	rat22	password

令人吃惊的是，这张小小的列表准确地揭示了口令的本质。我可以给你一个包括1000个甚至100万个口令的列表，但是你不会比在这张小小的表中发现更多有关口令的知识。

我知道这些口令的本质，因为我已经做过仔细地研究。几年来，我已经从各个渠道收集了生活中的口令。我已经收集了近400万个口令，而且我通常利用一些自动工具，例如Google这样的搜索引擎，在网上查询口令，这样一来，我的口令列表还在不断的扩大。我收集这些口令就是想更好地了解人们是如何设置口令的。五年来我一直在收集、研究，并关注着那些口令，其中有成千上万的“QWERTY”和“12345”。

我完全没有什么惊人的发现。口令越来越多，但并没有改变我对这些口令的统计，我选择出来的始终是那些。在前500个口令中，它们的长度、复杂性都几乎相同，并且几乎没有什么变化。

事实上，我得出的数目跟几十年前的那些研究非常接近。这些口令一个又一个被预测到是类似的：以一个或两个数字结尾、以几个数字开头、或是纯数字的、爱人的名字、日期、车名、运动队名，或是关于流行文化，或者是经常出现的“letmein”和“password”的形式。我可以另外再收集400万个口令，但得出的结论将可能会是一样的。

你并没有那么聪明

在口令方面，有个事情一直困扰着我，那就是：很多人都认为他们是聪明的或独特的，然而，事实上并不是。如果你看到100万个口令，你可能会惊奇地发现，你的口令跟其他很多人的口令都很相似。如果你曾经有过一次穿越美国大陆的长途飞行，你可能会注意到：除了那几千平方公里的空地，你并没有看到很多其他特别的东西。偶尔，你会经过一些名胜古迹，但随后又会回到一片空地。

这跟我在研究口令时所看到的情况非常相似。成千上万个口令都无外乎是那么几个类似的形式。虽然可以选择很多形式的口令，但是很少有人用到。

这些年来，我开始根据格式对口令进行分类。以下是一些最常见的几类口令书写格式，这些例子都是我们不应该采用的，永远不要按照这样的格式来设置口令。