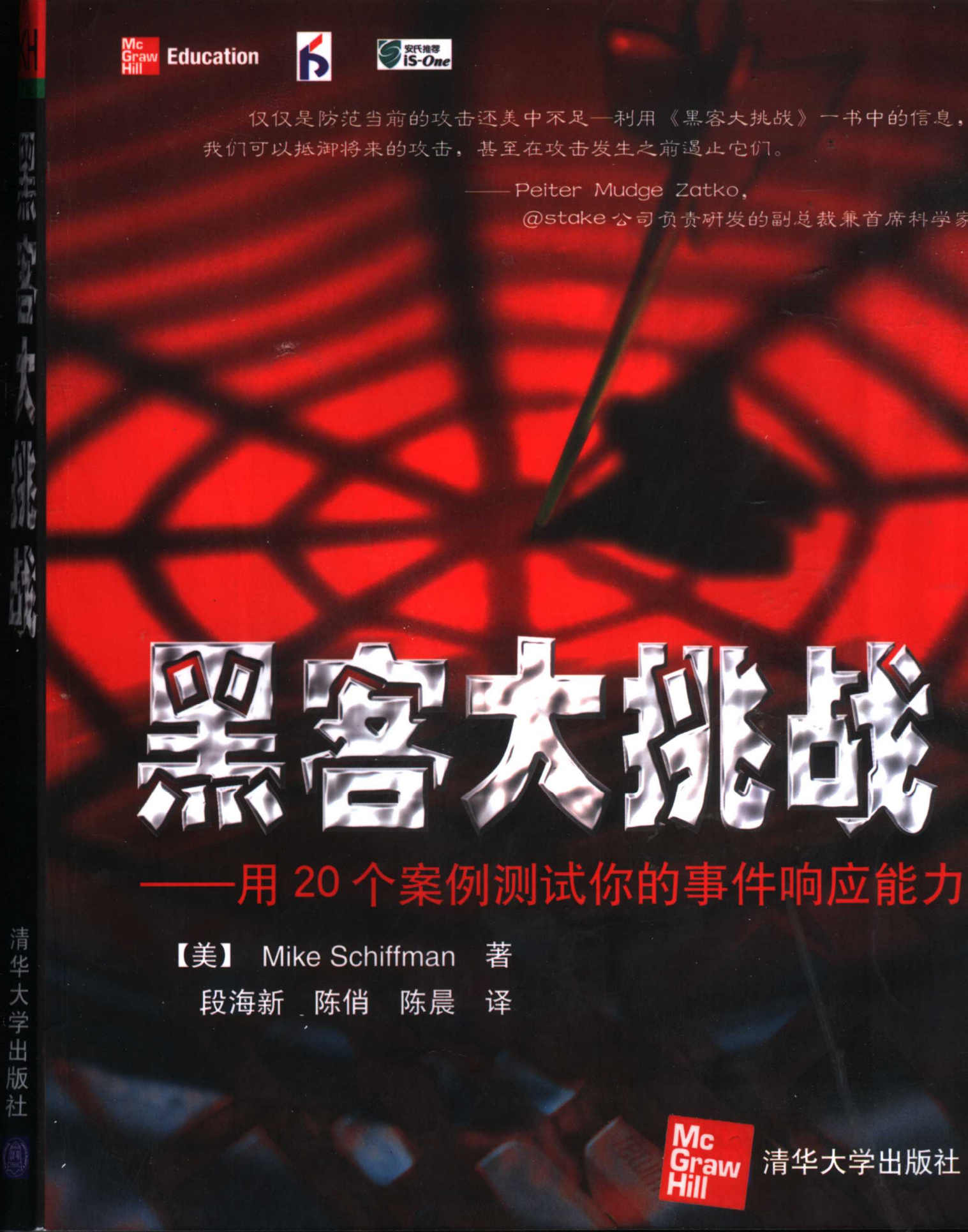
Mc Graw Hill Education
安氏推荐 iS-One
仅仅是防范当前的攻击还美中不足—利用《黑客大挑战》一书中的信息，我们可以抵御将来的攻击，甚至在攻击发生之前遏止它们。
——Peiter Mudge Zatko，
@stake公司负责研发的副总裁兼首席科学家
黑客大挑战
——用20个案例测试你的事件响应能力
【美】 Mike Schiffman 著
段海新 陈俏 陈晨 译
清华大学出版社
Mc Graw Hill
清华大学出版社

黑客大挑战

——用20个案例测试你的事件响应能力

【美】 Mike Schiffman 著

段海新 陈俏 陈晨 译

清华大学出版社

（京）新登字158号

北京市版权局著作权合同登记号 01-2002-3394
EISBN 0-07-219384-0

内容提要

当今，恶意的黑客几乎无处不在。该如何把他们拒之于你的网络之外呢？本书用高级安全专家们所提供的20个真实的攻击实例，全面展示了黑客事件的攻击过程及解决方案。

全书分为两部分，第1部分包括20个挑战，其中囊括了安全领域中的重要专题，包括拒绝服务攻击、无线技术、Web攻击、恶意代码。每个挑战包括一个详细的事件描述——入侵是如何检测到的、证据和可疑的线索（诸如日志文件和网络图等），以及要解决的一系列问题。然后，在第2部分，将给出针对每个挑战的解决方案，从中你将看到专家级的事件分析、问题解答，以及预防和缓解措施。

本书适合于安全管理员和网络管理员，企业及组织的政策制定者也会从中受益。

书　名：黑客大挑战——用20个案例测试你的事件响应能力
作　者：Mike Schiffman
译　者：段海新　陈俏　陈晨
出版者：清华大学出版社（北京清华大学学研大厦，邮编100084）
印刷者：北京耀华印刷有限公司
发行者：新华书店总店北京发行所
开　本：异16　　印张：22.875　字数：439千字
版　次：2002年10月第1版　　2002年10月第1次印刷
印　数：0001~6000
书　号：ISBN 7-302-05733-8/TP・3385
定　价：38.00元

序

“《黑客大挑战》以它的对“从重点入手”事件响应的场景，的确向那些即使是技术上最精明的IT安全高手挑战。这些源于现实的案例，是从许多领域最有经验的从业者的许多故事中精选出来的；成堆的原始日志数据，可以测试人的分析技巧；书中的分析技巧非常犀利，以至于能分析至这些烦人的日志的最后一行。”

——Joel Scambray,Foundstone公司的管理负责人，畅销书《黑客大曝光》和《Windows 2000黑客大曝光》的作者（这两本书已由清华大学出版社出版）

“《黑客大挑战》读起来就像是充满挑战的神奇小说，它提供了实际的例子和方便的提示，而这对于学习怎样去调查计算机的安全事件是至关重要的。”

——Kevin Mandia,Foundstone公司计算机法律事务的主管

知彼知己，百战不殆

——孙子

B

安 氏 推 荐

——潘柱廷

这本书从系统拥有者的角度，面对攻击和入侵事件、面对纷乱的头绪，教导我们如何从中发掘关键问题和关键要素，并最终解决问题。

如果你是对黑客攻防技术非常了解或者非常感兴趣的读者，则可以从书中找到很多的技术细节。而且还可以挑战一下自己，看看自己能否从前面的“挑战N”中分析出“解决方案N”。

如果你对这方面技术不太熟悉，则可以通过浏览全书、回避技术细节去体会解决安全问题的要旨。你会发现很多问题都会涉及、甚至最终归结到管理问题。从中我们也同样可以获得教益。

如果你读过全书，也许你会和我（们）一样在下面几个方面产生共鸣：

- ▼ 一定要打上最新的补丁，升级最新的系统；
- ■ 日志一定要开启，而且要适切地得到保护（几乎所有的案例，能够最终追查出结果都是通过各种各样的日志帮助实现的）；
- ■ 无线网络非常不值得信任；
- ■ 不要将没有加固的系统放到网络中（更不要放到防火墙外），这是非常愚蠢的；
- ■ 用户帐号和口令是永恒的问题；
- ■ 防火墙和入侵检测IDS都是非常有效的安全措施；
- ▲ 三分技术、七分管理……

这本书，建议读者最好能够读两遍。然后，将你所在机构出现的安全问题也用这种方式记录下来，会非常有意思，而且非常有意义。

关于本书的主笔

Mike Schiffman，CISSP(认证信息系统安全专家)，@stake 公司安全架构的负责人，@stake 是专业安全服务的主要提供商。他已研究和开发了许多前沿技术，包括像 firewalk 和 tracerx 这样的工具，还有到处使用的低层的数据包整形函数库（packet shaping library），libnet。他还在一些事业机构和政府部门做过报告，例如NSA（美国国家安全局），CIA（美国中央情报局），DOD（美国国防部），AFWIC，SAIC 和军情处。Mike 已在<Software Magazine>和<securityfocus.com>上发表过多篇文章，参与过《黑客大曝光》一书的编写。

关于本书的技术评论者

Tom Lee（MCSE）是Foundstone 公司的IT 经理。他的工作是保证Foundstone 的系统正常运转和阻止入侵者的攻击。Tom 在系统和网络管理方面有数十年的工作经验，他维护过许多不同的系统的安全，从Novell 网，Windows NT/2000 到Solaris、Linux 和BSD。在加入Foundstone 公司之前，Tom 在加州大学担任IT 主任。

D

这是我的第一本书，特别献给两个人：第一个是我去世的父亲，是他当初点燃了我胸中对计算机浪漫主义的火焰；其次是我迷人的女友，Alisa Rachelle Albrecht。

引　言

黑客攻击 Cal-ISO

2001年6月9日，DAN MORAIN，*Los Angeles Times*资深作家

SACRAMENTO(美国加州首府)——The Times得到的一份机密报告表明，在至少17天的高度能源危机中，黑客对加州的首要电力传输计算机系统发起了一次攻击。

尽管攻击的成效非常有限，但还是使得这次计算机攻击的目标——加州独立系统操作平台Cal - ISO——在计算机安全方面出现轻微的失误，这个平台监控着加州大多数大规模的电力传输网。

Cal - ISO的官员说失误已经改正，对电网不再构成威胁。但是其他了解这次攻击的人士透露，黑客差一点就获得对系统的关键部分的访问权，并且可能严重破坏贯穿全州的电力传输。

共和党和民主党立法者对像加州能源系统这样一个基本的部分出现安全缺口都非常恼火。有人称这次攻击为“凶兆”。

一份被标记为“机密”的内部机构报告表明，这次攻击早在4月25日就开始了，然而直到5月11日才检测到。这份报告上说，主要的攻击是某人从中国广东通过中国电信的途径发起的。

这份报告上还说，黑客除了使用中国电信计算机系统，还利用位于北加州Santa Clara和Okla州Tulsa的Internet服务器进入系统。James Sample，提交这份报告的Cal - ISO计算机安全专家说，他无法确切指出攻击者位于哪里。

Sample说：“你不知道那些人真正来自哪里……一个野心勃勃的美国黑客可以假装成一个中国黑客。”

这次入侵发生在中国军用喷气式飞机与美国间谍飞机相撞之后的那段中美关系紧张时期。在5月初，许许多多公开报道的计算机攻击很明显是从中国发起的。大多数那些事件都包含一些恶作剧；并用反美的标语涂改政府的网页。

如果黑客设法侵入在Folsom（Sacramento东部小镇）的总部的计算机，对Cal - ISO计算机系统的攻击显然存在潜在的更严重后果。那儿连接着一个系统，控制着贯穿加州的供电系统。整个加州可以说被捆在美国西部的电力传输网上。

L

据熟悉这次攻击的 Cal – ISO 内部调查人士透露："这次入侵几乎酿成灾难。"

5月7日和8日，当入侵正在进行时，加州许多地区大面积地轮流断电，但星期五 Cal – ISO 官员说黑客攻击和断电之间没有必然联系。这次断电影响了 40 多万正常用户。

报告说，攻击被发现后，调查员找到了黑客试图"编译"或编写软件的证据，这个软件可使他们得到所谓防火墙保护下的计算机系统的更多敏感信息。

–摘自 *"Los Angeles Times"*

报纸不断用与上面类似的故事来轰击我们，充斥着世界各地计算机系统被恶意个人广泛滥用的报导。在 2001 年的夏天，cnn.com 在 3 个月内做了个简单的问卷调查，调查表明人们关心的文章标题如下：

- ▼ 新的侵略性蠕虫威胁计算机用户
- ■ 黑客迫使银行取消 Visa 记帐卡
- ■ 新病毒通过 Adobe Acrobat 文件传播
- ■ 俄罗斯黑客被拘捕
- ■ 谁在读取你的即时短信息?
- ■ 五角大楼称每天都遭受计算机攻击
- ■ 分析家：任何网站都可能成为攻击目标
- ■ 中国警告大量的黑客攻击
- ▲ FBI 发出拒绝服务（Denial of Service）警告

事实上，随着 Internet 规模和用户的增长，计算机安全事件也在增长。新闻无法告诉我们这些事件是怎么发生的，什么导致了这些事件？什么激发它？什么驱使它？怎样能预防它？如何能使危害减小到最低程度？而最最重要的是，事件是怎么发生的？假如你对这些有兴趣的话，这本书最适合你不过了。

《黑客大挑战》这本书带给你现实中的计算机安全战争故事，这些故事来自于当前从事计算机安全行业中顶尖的研究者、顾问、事件响应专家和取证分析师。然而，此书不仅仅是复述这些故事，而是将读者置身于故事当中。当每个故事展开的时候，事件的相关信息将呈现在你面前，并由你来解决这个案例。

本书和其他随手可得的书不同。各个行业的网络管理员和网络安全工作者都可以从书中看到类似企业被侵入的真实场景。他们可以通过本书学到有必要关心的各种情况和应付一些攻击者的方法。另外，本书的幽默风趣也值得一读。

组织

本书分为两个部分。第1部分包含了所有的案例研究或者说是挑战。在每个挑战中都有详细的案情描述和取证信息（如日志文件、网络拓扑图等），这对确定究竟发生了什么很有必要。出于简短起见，书中删除了大量的证据，留给读者的几乎都是特有的关键信息（这样读者可以不必历尽辛苦去读一页页原始数据了）。在每个案例研究的末尾，有一些精心准备的问题，引导读者正确地进行取证分析。

本书第2部分包含了第1部分所有挑战的解决方案。这部分彻底研究案例，详细分析、解释所有的证据信息，并解答第1部分的问题。另外，还介绍了如何减轻危害和预防攻击。

保护无辜者

为了维护书中讨论的组织的隐私权，我们不得不改变或删减每个故事中的很多细节。由于非常慎重地保持了每个案例研究的完整性，因此在这个过程中没有失去案件的有用信息。改动的信息如下：

- ▼ 公司名字
- ■ 职员名字
- ■ IP 地址
- ■ 日期
- ■ 网页被黑细节（为了改变信息和删除那些不合适的内容）
- ▲ 没必要的故事情节

漏洞信息

在阅读本书时，我们随时都可能参考包含特定漏洞信息的外部资源（在每个解决方案后面查找“追加资源”部分）。下面两个机构，MITRE 和 SecurityFocus，都提供了大致相同的漏洞数据库，这些数据库是非常实用的资源。

MITRE（http://cve.mitre.org）是一个非盈利的国家技术资源组织，它为政府提供

系统工程、研究开发和信息技术支持。公共缺陷与漏洞（Common Vulnerabilities and Exposures，CVE）是一个列表或者说是一个字典，它为公众已知的信息安全缺陷和漏洞提供统一的名字。使用统一的名字可以使各自独立的数据库和工具更容易地共享数据，直至现在，这些工具和数据库还是不容易整合。这使得CVE成了信息共享的关键。

SecurityFocus（http://www.securityfocus.com）是最先进行商业安全信息服务的提供商。该公司管理着这个行业中最大的、最活跃的安全社区，在安全行业占统治地位，它每个月为超过25万的独立用户提供服务。SecurityFocus的漏洞数据库是任何已公布的计算机安全漏洞的最完全集合。

复杂性分类

描述每个挑战的复杂度有3个级别，列在每个挑战开始的表格中。这些级别包含了事件的攻击者操作难度和安全人员预防复杂度两个方面。

攻击难度

攻击难度是指攻击方需要的技术能力级别。这个级别可以概括攻击者全面的技巧。我们通常知道，一个平台越是复杂和安全那么攻击者要攻破它就越是困难（当然，也有例外）。

- ▼ 低　在这个级别的攻击通常是一些现成的脚本程序攻击。攻击者所做的仅仅是运行一段攻击脚本程序，编译一些常见的代码或者使用一个众所周知的攻击方式，显现出少许新意或根本就没有创新。这是最容易上手的。
- ■ 中等　攻击者使用了公众了解的攻击方式，但是扩展了攻击并创新了一些超越原版文件的东西。这种创新可能是地址伪造，或者有少许超出常规的攻击性能上的改动。
- ■ 困难　攻击者非常聪明并且技术相当娴熟。攻击者利用的漏洞可能已经公布也可能没有，并且攻击者很可能编写他（她）自己的程序代码。
- ▲ 极难　这种规模的攻击通常表现为此领域的专家水准。攻击者技术非常娴熟，利用的是未公开的漏洞或最前沿的技术。攻击者也被迫作出大量创新，并且假如适用的话，可以将他或她的攻击记录掩饰得很好且留下非常隐蔽的后门，以便以后再次进入。除了碰到老到的安全管理员或自己倒霉外，通常很难抓到这种攻击者。

预防和缓解的复杂性

预防复杂程度是针对某个组织在防止事件发生时所需的复杂性级别而言的。缓解复杂程度是通过利用组织现有设备减轻事件危害的冲击所要求的复杂等级。它们两个非常近似，所以被定义为同一个类:

- ▼ 低　预防或缓解这类问题可能只是简单地安装一个软件补丁或进行软件升级，或在防火墙上加一条规则。这些更改通常非常简单，不用费很大的努力就能做到。
- ■ 中等　除了在防火墙上策略的改变外，可能还要安装一个复杂的软件补丁或软件升级。重装被攻破的机器和／或对基础设备进行改动也是必要的。
- ▲ 困难　除了主要的基础设备需要改变外，还需要安装一个复杂的补丁，或者一次给很多机器进行一系列的升级。总而言之，这个等级也包括了那些极难彻底预防或缓解的漏洞。

本书中使用的一些约定

除了挑战之外，你还应当了解这本书是如何设计的。这儿是一个概要。在每个章节的正文中你将发现很多日志文件、网络拓扑图、文件列表、命令输出信息、代码和各种各样其他的取证证据。这些信息尽可能地排版成与原始的信息相同，但是考虑到版面的限制和出于保密缘故，我们做了一些必要的改动。

本书分成两个部分。第1部分，挑战1~20呈现了真实事件的细节。每个挑战的开始都有一个总结表，在表格中列出了受害公司的行业和攻击、预防及缓解的复杂度级别。

问题

在每个挑战的末尾，你将看到到一系列问题，这些问题将引导你去搜索事件的细节并指导你找到全面的解决方案。在解决这些挑战时，你可以随意地在这个部分做笔记或者写下全部答案。

答案

在本书的第 2 部分中，你将看到相应的解决方案 1~20。解决方案解释了如何解决事件的细节，还回答了本书第 1 部分提出的问题。

预防

解决方案中包含了预防部分，对黑客的攻击，你将看到一些如何防范于未然的建议（对那些与本书描述的不幸组织情况相似的公司，这项内容非常有用）。

缓解

解决方案同时也包含了缓解部分，从中你可以学到受害公司在遭到攻击之后如何尽力使损失降至最小。

线索

你可能发现一两个有助于你解决挑战的线索，但是在最关键的部分还得靠你自己。

祝你好运！

目　录

F

H