

◎ 藐视网络秩序的电脑人

黑客案例

// 麦赫 著
aihe

巡游五角大楼，登录克里姆林宫，进出全球所有计算机系统，摧垮全球金融秩序和重建新的世界格局，谁也阻挡不了我们的进攻，我们才是未来世界的主宰。

—— 凯文·米特尼克

“最让我束手无策的商业对手便是那些隐藏在网络后面的黑客”

—— 比尔·盖茨

The hacker's cases

西南财经大学出版社

麦赫 著
aihe



黑客案例

西南财经大学出版社

责任编辑：任丕中

书 名：黑客案例

作 者：麦 赫

出版者：西南财经大学出版社

(四川省成都市光华村西南财经大学内)

邮编：610074 电话：7301785

排 版：西南财经大学出版社照排部

印 刷：四川五洲彩印厂

发 行：西南财经大学出版社

全 国 新 华 书 店 经 销

开 本：850×1168 1/32

印 张：14.5

字 数：320千字

版 次：1998年6月第1版

印 次：1998年6月第1次印刷

印 数：1—8000册

定 价：23.80元

ISBN 7-81055-324-0/T·10

1. 如有印刷、装订等差错，可向本社发行部调换。
2. 版权所有，翻印必究。

The hacker's codes

让所有公司束手无策的商业对手
未来世界的最高危机

“在未来的时代里，只有黑客能改变这个世界的^{所有}秩序，无论是经济秩序，还是军事秩序。”

——德国《快捷报》

CONTENTS

第一部 挑战美国

(I)

☞ /今天威胁着美利坚合众国的，绝不是什么共产主义大国，而是一个人或者一个隐形群体——

☞ /“能摧毁别人的经济体系算什么，我可以让所有国家的军事部署在一夜间化为乌有，可以让所有武器试验室、科学试验室、工业试验室的苦心经营体无完肤，我可以让美国再花几十亿重新部署他们的导弹、潜艇和军队。”

☞ /一个敢向美国叫板的电脑人。

☞ /重要案例——

·当提示符稍作闪烁后，伍德所熟悉的画面并没有在屏幕上出现，取而代之的竟是一双血淋淋的眼睛！……这张北美最为核心的“北美防空系统布防图”上，已经被堆满了白骨，涂抹上了鲜血，在图中央，赫然写着“你们这些臭狗屎！”

·除了总统府五角大楼外，还有谁知道美国所有指向天空，指向苏联及其盟国的核弹名称、数量和位置。

·当一个黑客高手接触到一套系统软件的时候，对他最有吸引力的肯定是防御功能。……米特尼克改动后的程序已经变得简洁明了，它使得其中的联系更为快捷，工作效率大大提高，而设置的保密措施极为巧妙——这就是一个黑客的另一种价值。

目 录

·突破太平洋贝尔公司的洛杉矶控制中心,所带来的登录的巨大方便和本身的诱惑,是没有任何黑客所能抗拒的。

·“枪炮与玫瑰”给他所带来的强大的破坏欲望,使她看到了这个黑客的可怕。

·“勇士们,出发了!”——米特尼克、金斯博格、凯斯迪沃兹的贝尔公司窃案!

·传统黑客意味着对完美程序的高尚追求,他们的兴趣所在是不断发现程序中的缺陷。改变了世界的比尔·盖茨曾经就是这一类黑客。

·有人指控他非法闯入电话公司的维修系统和计帐计算机,并使用从商务卫星系统窃取的口令拨打长途电话,同时还有无线电业余爱好者协会指控其闯入该机构的通讯频率……

·在太平洋贝尔公司洛杉矶中心计算机上建立帐户,那样可以发出指令,为所欲为——但当他控制了洛杉矶地区的电话系统后,他却没有使用他所掌握的权力。

·1986年4月,米特尼克渗入休斯公司的计算机系统,这使得他成功地进入了国家计算机安全中心……

·“如果你不介意的话,就把这个帐号取名为‘黑客’吧。”米特尼克向他的追踪者发出了挑衅。

·对手似乎想修改 XENIX 文件,这个 UNIX 文件的升级版是圣特·克鲁兹公司的商业核心机密,更让人震惊的是,他显然想拷贝 XENIX 文件。

·他扬言可以在很远的地方通过“逻辑炸弹”摧毁任何计算机系统。

·他已经明白,那两个年轻人已经把皮埃尔斯大学新开发出来的软件在磁盘上作了备份,这个 CP.COM 执行程序已经把这份价值……

·他出售的这种逻辑炸弹可以摧毁公司的工资报表、库存数量及销售情况登记,让公司管理陷入彻底的混乱之中。一时间,那些仇恨公司的雇员竟对……

……她知道,这是那个黑客的手段,因为他曾发誓要报复那个讨厌的司法人员,他对她家的电话……

目 录

- 米特尼克又通过埃尔·锡甘多的休斯雷达系统集团闯入……
- 斯坦利·里夫金怎么能够利用计算机系统盗走太平洋平安银行 1000 万美金？——一场没有暴力的抢劫！
- 现在，数据设备公司最重要的软件——新版本的 VMS 系统正成为米特尼克新的登录对象。
- 1988 年，马里兰州帕图森特海军站又被米特尼克——
- 尤金·科斯特曼不得不承认，入侵者相当聪明，他们修改了 VMS 操作系统，修改了管理用户登录的程序，每次用户登录进入系统时，程序就会自动把登录口令拷贝到一份隐含的文件中，而且入侵者还在……
- 美国航天局在 1988 年举办了一个国际研讨会，邀请众多国际有名专家，目的是联手对付试图入侵航天局计算机系统的 Hacker……
- 他发现，这个黑客每一次入侵后，计算机硬盘空间便迅速缩小，有一次就会缩小相当于几十本教科书内容的 40 兆个字节，居然在硬盘上没有产生新的文件，那么这些文件被他藏在了哪里呢？
- 有人窃取了公司的源代码！这个被数据设备公司视若珍宝的文件在多种安全措施的防范下是怎样被窃取的呢？
- 特洛伊木马程序看似是无害的文件，但它可以用来盗取口令甚至摧毁系统数据，而系统管理员却很难发现系统内发生的变化。是谁安装的这个“木马”——
- 是谁闯入这个世界上第二大电脑制造公司，偷走了他们最引以为自豪的 VMS5.0，是商业对手还是……
- 他喜欢在计算机系统上旅行，他只需敲打几个键，就可以拥有全世界所有计算机，拥有所有机密或绝密的文件——工业、金融、甚至军事，但他还是最喜欢浏览阿帕网……
- 当轻松网络把 25 个国家 34,000 台数据设备公司的计算机连接在了一起之后，这里便成了所有黑客向往的“理想乐园”……
- 他们在联邦家庭信贷银行办公楼的地板下找到大型电话线控制箱，然后把 UA 调制解调器接在电话线上，接着就开始——

第二部 平衡计划

(191)

👉 /他无所不在,无所不能!——一个比索罗斯更雋智,更具杀伤力的智者!

👉 /平衡东西方,帮助落后的国家追赶超级大国,缩小所有商业对手的差距,使世界两大集团在军事领域保持均势,让所有工业、科技、军事、通讯、大至于世界……这就是我潘戈的思想。

👉 /威胁全球的登录碎片……

👉 /“你们俄国人想到什么,我就能让你们得到什么——阿尼斯顿陆军军械库的装备材料,行不行,红宝石导弹基地的呢?”

👉 /“我控制了他们的航天飞机……”

👉 /重要案例——

·潘戈略带骄傲地回答说,他是 60 年代西柏林左翼运动的产物,并对戈尔巴乔夫正在进行的改革持支持态度。

·这张磁盘上拷贝的是 DEC 的计算机安全程序;这对苏联人来说绝对是……

·“你真是一个天才,居然为我搞到了 CAD 软件和 CAM 软件……”

目 录

·“我可以在计算机网络上周游世界,从西柏林到洛杉矶要不了几秒钟,进出国外的计算机系统也就是眨眼的功夫。”

·“如果有一台高速的调制解调器和一台高配置的计算机,外加足够大的硬盘空间,我就一定能办到……”

·对于潘戈来说,政治和种族问题是无关重要的,黑客活动既是手段,也是目的……

·巴尼莫为他展示了从迪姆网上窃取数据的手法……

·潘戈编写的这个循环程序,象是一个连锁信,它可以先对自身复制两个备份,然后每个备份又变成两个,如此循环不止,这就是耗尽直线加速器中心的计算机资源的最有效的方法——

·CERN,一所国际性高能物理研究所,由 14 个国家的科学家组成,连这样的地方居然也成了黑客们消磨时光的场所……

·“不,我是一名黑客,不是罪犯,也不是工业间谍!”

·每当他到达一台远程计算机,需要了解连接情况的时候,他就把音响连接器连在电话上,再配上喇叭,然后象使用收音机一样,用手拨动音响连接器的调谐频率,从喇叭发出的声音中辨别与远程计算机对接是否成功——

·NUI 可以敲开 X-P 数据网大门!

·一旦黑客在一台个人计算机上抢滩,他就可以在许多与此连接的机器上进行“网络巡航”,如果可能,黑客还会把它用作通往其它网络系统的跳板。潘戈发现,在不同的网络间交叉跳跃可以使他很好地……

·请看看 60、70 年代的麻省理工学院的传统黑客手法——

·他认为自己不过是个现代的罗宾汉,通过黑客活动,他们可以把计算机系统的安全漏洞暴露出来,并证实西德当局认为计算机系统无懈可击的错误观点。

·“混沌”俱乐部的年会上,无计其数的黑客突然冒出来,在这里,他们为我们展示了各个方面的登录才华——

·他们闯入了渥太华警局! 并且让……

目 录

·且看潘戈是如何在众目睽睽之下侵入太平洋彼岸的数据设备公司，用 DCL 语言编写程序，设置电子公告牌的……

·“赖特斯特利 511 黑客组织的安全报告”。

·海格巴德认为计算机网络的威力是没有限制的，“逻辑炸弹”的能力足以使黑客登上主宰世界的权威地位。

·“VAX 霸主”黑客俱乐部试图邀请他加盟，以便能在……

·当他建立了特权帐户后，计算机就完全置于他的控制之下。“我可以阅读或者修改其他用户的文件，翻看他们的电子邮件，使他们的工作毁于一旦……”。“而我有时还要给它们安上臭虫程序。”

·黑客活动最具魅力的地方在于他人侵入一个未知的系统前，他是……

·NASA 黑客事件——控制美国最先进的航天飞机！

·他窃取了 XWINDOWS 软件和 GNU 依码克斯程序！——

·被称为“有魅力的毒蛇”的巴劳案情——

·美国的“攻击性软件开发部”开发的产品被这个黑客称作“软件战争”，它的杀伤力只有黑客才能终结它……

·最负盛名的计算机安全专家对面坐着的居然是屈指可数的黑客高手——且看他们的较量。

·他们担心克格勃会暗杀潘戈！。

·一个把鼻子伸进了欧洲各大机构的黑客居然被保加利亚索菲亚电子学院正式邀请参加座谈。

·潘戈的“三点战略”——第一，向苏联人提供黑客的关键技术，要价在 75000~150000 马克之间；第二，在共产主义国家举办黑客研讨会，向他们传授技术；第三，说服苏联人在东柏林为他们提供一套……

·他在新加坡的计算机上成功登录了，并找到一个被称作“安全包”的 VMS 操作系统安全程序，这个程序成了他送给对方的见面礼。

·他——列举了他曾经闯入过的系统，这些系统不论是名声还是影响，都足以让你……

·登录碎片——一个让自称全球第一的黑客看到后就改称为“西海岸

目 录

第一”的……。

·我可以给你们提供西德黑客的技术关键,包括几十台美国军事计算机的登录名和口令,但价格是……。”

·“中国在世界两大集团的较量中还算不上是十分重要的角色,所以我们平衡计划的目标是……

·“美国或者俄罗斯对我们来说毫无秘密可言……。”

·“我对黑客技术不感兴趣,我只想得到有关雷达技术、核武器和星球大战计划的资料,当然,如果你们给我 VMS、UNIX 的源代码、CAD 和 CAM 软件,倒还是挺有价值的。”

·黑客 S·K·斯多的原则是绝不进入劳伦斯·利沃莫尔实验室的系统。但这一次,他……

·我们是能够进入全球最敏感计算机的黑客;我们可以窃取任何机密的文件,并帮助任何人赶上他的商业对手,甚至帮助有些国家在技术上赶上西方,只有我们能够平衡这个世界……。”

·“我是汉诺威一个黑客组织的成员,我可以向你们提供一些有趣的信息”……

·这次参加“混沌”年会的黑客正在反复讨论一个新的……

·“BBC”称他为 VAX 霸主,但他却认为自己不过是一个……

·采访在晚上 9 点钟播出,有 300 万西德观众收看了这一节目——

·“我想黑客应该创造性地使用技术,而不是仅仅把操作计算机当作是一份工作。我认为,大多数先进的现代电脑概念都是由自称黑客的人发起和总结出来的”

·一个黑客的网上独白——他承认自己无法摆脱这一活动的原因。

第三部 蠕虫事件

(345)

3 / 一个连兰德公司这个举世闻名的思想库也无法预料

— 7 —

目 录

的入侵——“我们对此也束手无策……”

👉 /“既然它没有统治者，没有一个电脑沙皇坐在华盛顿建立秩序，统治一切，那就看我能不能成为新的亚伯罕姆·林肯。”

👉 /紧急，紧急！网络告急！蠕虫程序正在成为网络时代的“1999 恐惧”。

👉 /重要案例——

·拉普斯利发现这个名叫德曼的用户，正控制着一个程序，而这个小程序又隐藏在一大堆正在运行的程序之中……

·原来闯入者根本就不是人，而是一个……

·当他试图阻止对方入侵时，却发现……

·遭到袭击的系统速度越来越慢，并开始陷于瘫痪，而更怪的是，它瘫痪后居然会……

·谁也预料不到，11 月 2 日傍晚互联网会遭受如此重创。

·只要它一进入某台计算机后，它就会象生物病毒一样迅速传染。——它不停地复制了数百份拷贝，使机器运行速度越来越慢。同时，当它成功进入一台机器后，它又立刻转向下一个目标，这究竟是什么病毒？

·他们拒绝撤离网络，因为这意味着自己的失败，是谁迫使这些专家“玉石俱焚”？！

·这些流动的代码告诉专家们，病毒程序试图用一种被称为字典进攻的方法破解口令——

·“你们知道我是怎样攻入你们这个坚固体系的吗？你们这些猪

目 录

……”。

·显然波斯蒂克用在 E-mail 上发送处理病毒的办法,但是——

·这次入侵目标是美利坚合众国的武器实验室——劳伦斯·利沃莫尔实验室……

·父亲是联邦政府的电脑安全专家,儿子是才华横溢的黑客,且看这场知己知彼的……

·莫里斯在 M-209 上发明了一种绝妙的方法,它可以使……

·“我的网民有 400 万,我的机构健全——金融、军事、工业、医疗,我能真正的一触即发……

·一天晚上,一个出岔的蠕虫程序在帕罗·艾尔特研究中心的区域网上失去了控制。于是……

·CP 的又一次尝试——

·通过这一次登录,他赢得了“孤独的才华横溢的程序专家”的名声。

·他是怎样将病毒从 Unix 漏洞植入系统的……

·“我想我他妈的闯大祸了”,他看到这个系统后不禁惊呼——

·他建议再释放一个杀病毒程序,一路追踪并杀掉病毒,但是预想不到的是……

·他只轻敲了几下键盘,就不仅使成千上万台电脑也使自己的生活陷于了停顿。毁灭吧!让他妈都见鬼去吧!”

1 THE HACKER'S CASES

挑战美国

○今天威胁着美利坚合众国的，绝不是什么共产主义大国，而是一个人或者一个叫“凯文·米特尼克”的隐形群体——

○“能摧毁别人的经济体系算什么，我可以让所有国家的军事部署在一夜间化为乌有，可以让所有武器试验室、科学试验室、工业试验室的苦心经营体无完肤，我可以让美国再花几十亿重新部署他们的导弹、潜艇和军队。”

○一个敢向美国叫板的电脑人。

——《黑客案例》——

在所有的黑客中,凯文·米特尼克(KEVIN·MIT-NICK)是最具传奇色彩的人物。好莱坞甚至将他搬上了银幕。在他 15 岁的时候,仅凭一台电脑和一部调制解调器就闯入了北美空中防务指挥部的计算机系统主机。美国当局认为,只要他手中拥有键盘,就会对社会构成威胁。联邦调查局将他列为头号通缉犯,并为他伤透了脑筋。网络上的所有信息,都是他的囊中之物,但他却过着简朴的生活。他是真正的少年黑客高手。

引 章

艾休·伍德从未象现在这么兴奋,走进五角大楼时,大声与警卫打了个招呼,让那个还嫌稚嫩的小伙子竟有点不知所措。

伍德快步走向电梯,这时,电梯的门正徐徐关上。伍德高声叫道:“等一等!等一等!”并迅速挤进了电梯。“11 层。”伍德揪下了 11 键,转回头来,对电梯里的人微微一笑。

这时正是上班高峰时间,电梯里稍嫌拥挤。一个双手交叉胸前,抱着公文包的女少校看了伍德一眼,便收回了目光,将脸转向一边。伍德感到了自己的失态,把脸上的笑容紧了紧。但这并不妨碍他的好心情。

当普通职员的日子总算熬到了头。对于已经在五角大楼供职二十多年的伍德来说,深知“北美空中防务指挥部电脑部主任”的头衔意味着什么。一想到很快就要登上这个梦寐以求的宝座,再也不用看“老东西”艾博拉的脸色,忍受他那张冒着胃气的臭嘴在耳边大吼大叫,这个漂亮娘们儿的白眼又何足道哉!



电梯在 11 层停了下来。伍德走出电梯，在办公室门前刷完身份卡后，做了两个深呼吸，让心情平静了一下，便推开了办公室的大门。

“老东西”艾博拉显然还没有来进行他例行的“早间巡视”，埃比克和沃尔特手里端着咖啡，正在聊着天。

“早上好！”

听见开门声，沃尔特回过头来跟伍德打了一个招呼，还没等伍德做出反应，便又投入与埃比克的对话中去了。

“毛头小子！”伍德心里暗骂，我与你们这些垃圾在这个办公室里已呆不了几天了。当我搬进主任的单间后，你们对艾博拉的敬畏会全部转移到我这儿来的。

伍德倒了一杯咖啡，在电脑前坐了下来。打开电源后，看着屏幕上的显示。

请输入密码：

伍德闭着眼睛也能敲出正确的密码。他对这套系统比对他老婆身体的各个部位还要熟悉。

“MAYFLOWER(五月花)39873”。

密码输入正确，请稍候……

“欢迎进入北美空中防务指挥系统(WELCOME TO THE NAADC)。”伍德口中念念有词，这正是下一个界面将要显示的内容。

但在提示符稍作闪烁以后，伍德所熟知的画面竟没有在屏幕上出现，取而代之的，竟是一双血淋淋的眼睛！

伍德登时目瞪口呆。