科爱传播
KEAI COMMUNICATIONS

No Tech Hacking

A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing

菜鸟也能防黑客之非技术攻击

Johnny Long　Scott Pinzon　著
李立新　周雁舟　李　新　译

科学出版社
www.sciencep.com

ELSEVIER

● 权威实用，著名黑客Kevin Mitnick倾情推荐
● 深入浅出，翻垃圾箱，跟踪尾随，背后偷窥等看似没什么技术含量的方法却是黑客重要的攻击武器
● 知己知彼，十大方法应对非技术攻击

No Tech Hacking

A Guide to Social Engineering, Dumpster Diving,

and Shoulder Surfing

菜鸟也能防黑客

非技术攻击

Johnny Long Scott Pinzon 著

李立新 周雁舟 李 新 译

科学出版社

北 京

图字：01-2008-5115 号

图书在版编目（CIP）数据

非技术攻击：菜鸟也能防黑客/（美）龙（Long，J.）著；李立新，周雁舟，李新译. —北京：科学出版社，2009

ISBN 978-7-03-025085-8

Ⅰ.非… Ⅱ.①龙…②李…③周…④李… Ⅲ.计算机网络–安全技术
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2009）第 127815 号

责任编辑：田慎鹏　霍志国　田　伟／责任校对：李奕萱
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

源海印刷有限责任公司印刷

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：15 3/4
印数：1—4 000　字数：373 000

定价：38.00 元

（如有印装质量问题，我社负责调换〈明辉〉）

作 者 简 介

本书的收入将用于 AOET，一个为非洲的艾滋病孤儿提供食物、教育和医疗的组织。它不仅仅是一个援助组织，AOET 的目标是在非洲撒哈拉地区打破贫困和绝望的循环，通过技能培训计划，无论儿童和成年人都能够自食其力，恢复身体健康，重塑对美好未来的希望。通过我在亚马逊网站的关联账号（详见我的个人网站或通过 http://tiniuri.com/f/Xpc）每购买一本书，相应就会为 AOET 捐赠一笔钱，而这些钱足够向一个孩子提供一个月的食物。其他零售（大约占一半的收入）将通过一个联合基金为儿童提供教育、食品和医疗服务。由于我被称为“照顾绝望中的孤儿和寡妇”的人，并且我的个人经验知道这将发挥多么重要的作用。当哈姆雷特感叹：“生存或毁灭，这是个值得考虑的问题！默然忍受命运暴虐的毒箭，或是挺身反抗人世无涯的苦难，通过斗争把它们清扫， 这两种行为，哪一种更高贵？”的时候，他的价值也得到了提升。

我是 Johnny，我是黑客！

此时此刻，我想感谢很多人，而现在又不能当面致谢，但将尽我最大的努力。首先，感谢上帝在我生命中的许多祝福。以基督为榜样，上帝的精神鼓励我以真正的价值观渡过每一天。这本书更多的是上帝的事而非 Johnny 的事。感谢我的妻子和四个孩子。言语无法表达我对你们的爱，感谢你们还我一个真正自己。

我还要感谢 Shmoo 工作组的成员和我的编写团队：Alex, CP, Deviant, Eric, Freshman, Garland, Jack, Joshua, Marc,Ross, Russ, Vince and Yoshi，他们为本书付出了许多心血。感谢你们的支持，特别是在这样紧的时间内。也要感谢 Scott Pinzon，作为一个优秀的编辑和团队成员。您教给了我很多。我也要感谢 Vince Ritts，是您启发了我，在我心中播下非技术攻击的种子。

同时许多朋友和粉丝的支持是我多年工作的动力，再次表示感谢。

请务必访问我们的服务网站http://notechhacking.com，因为我们将继续讲述有关非技术攻击的故事。

Johnny Long 是一个虔诚的基督徒、一个经过培训的职业黑客、一个冷血的海盗、一个训练有素的忍者、一个安全方面的研究员和作家。你能在他的网站(http://johnny.ihackstuff.com) 找到他。他是 Hackers For Charity (http://ihackcharities.org) 创始人，一个为以慈善为目的的黑客提供工作机会的团体。

技术编辑

Scott Pinzon CISSP 是 LiveSecurity 的主编，一家位于西雅图类似 WatchGuard Technologies 的公司。在其任职期间，他为 LiveSecurity 的 4500 多订阅者编辑、撰写和出版了 1500 个安全警告和最好的解决方法。他已经在安全加密产品、电子商务、语音消息等领域具备了 18 年的经验，由他共同创作和指导的发布在 Google Video 和 YouTube 网站上的 LiveSecurty 培训视频的点击量已经超过了 100 000 次，他也是 *Stealing the Network: How to Own a Shadow* 的编辑。

合 作 者

Jack Wiles 是一个在计算机安全、灾难恢复和物理安全等安全领域有 30 多年经验的安全专家。他还是一个专业的安全培训专家，在一系列有关计算机犯罪有关的主题上对许多联邦机构律师、公司法律顾问代理和内部人员进行了培训。他是一位打上“国土安全”标签的一系列安全领域方面的先驱者。1988 年以来，有 10 000 多人听过他的演讲。他还是 TrainingCo 公司的创办人之一和总裁，并与多家执法机构保持密切接触，尤其是美国的国家安全部门，包括联邦调查局、海关、司法部和国防部，还与其他许多防止高技术犯罪的人员保持密切联系。他还被指定为 North Carolina InfraGard 公司的第一任负责人，该部门已经成为美国最大的公司之一。他也是美国安全服务南卡罗莱纳电子预防犯罪任务组织的创建者之一和核心成员。

Jack 还是一位越战老兵，曾经在 101 空降师于 1967—1968 年在越南服役。他最近刚从陆军退役并保留陆军中校的军衔，在其陆军生涯的最后七年，他被直接指定在五角大楼工作。业余时间，他还是数家杂志的特约编辑。

序 作 者

拥有从事计算机安全行业超过 15 年的经验，Kevin Mitnick 是一个自学成才的专家，发现了复杂操作系统和电信设备的许多弱点。作为一个青年人，他喜欢钻研损害计算机安全的方法、策略、技术，对学习计算机系统和电信系统的工作原理也乐此不疲。

在构建自己的知识体系过程中，Kevin 曾经对某些全球著名公司的计算机系统进行了未经授权的访问，并渗透进入了已经开发的许多更具抗攻击能力的计算机系统。他曾使用了技术和非技术的方法获得了各种操作系统和电信设备的源代码，以研究其脆弱性以及内部工作机理。

作为世界上最著名的黑客，Kevin 成为全球许多报纸和杂志文章中的主题，他作为嘉宾参加了许多的电视和广播节目，对信息安全的相关问题提供专业咨询。除了出现在当地的网络新闻节目中，他还出现在 60 Minutes, The Learning Channel, Tech TV's Screen Savers, Court TV, Good Morning America, CNN's Burden of Proof, Street Sweep, and Talkback Live, National Public Radio 节目中，并且在 ABC 的间谍剧“Alias”中客串演出。他还在许多行业事件中做主题发言，是每周在洛杉矶播送的 KFI AM640 节目的主持人，在参议院作证，为哈佛法学院上课等等。他的第一本畅销书：《欺骗的艺术》（*The Art of Deception*）2002 年由 Wiley and Sons 出版社出版，其第二本书《入侵的艺术》（*The Art of Intrusion*）于 2005 年 2 月出版。

其 他 作 者

Alex Bayly 的生活十分接近普通人，尽管在其妻子的鼓动下，他曾做过一些社会工程学方面的工作。这使得他收集了很多的无用的和无意义的人 ID 卡。目前，作为英国的高级安全顾问，他从事社会工程学和传统的渗透测试。

CP 是 DC949 的一个活跃成员，也是每年公开的网络攻防竞赛 Open CTF 的组织者之一，尽管其正式职业是软件构架师，而他真正的爱好在于信息安全。他开发了一系列的开源安全工具，并在浏览器安全方面继续其研究工作。目前其主要忙于网络攻防竞赛 Open CTF 的扩展和丰富大家的知识。

Matt Fiddler 领导一个财富 100 强公司的威胁管理团队，他对规避锁技术的研究已经导致了数个锁设计缺陷的公开披露。他在海军陆战队时便开始做情报分析员，1992 年加入商业公司。最近，他把主要经历放在 UNIX 和网络工程、安全咨询和入侵分析方面。

Russel Handorf 目前在一家著名的证券交易所做高级安全分析员，也在 FBI Philadelphia InfraGard Chapter 的讨论会上做指导。在此之前，Handorf 为美国联邦政府、州政府、司法部门、相关公司及教育机构做安全顾问，负责培训、安全监察和安全评估等工作。

Ross Kinard 是 Lafayette 高中的学生。他对各种各样的坏点子和物理安全都非常感兴趣，从气筒到撬锁工具等事物都能让乐在其中。

Eric Michaud 是 Argonne 国立实验室脆弱评估小组的电脑和物理安全分析员。他是 The Open Organisation Of Lockpickers (TOOOL) 美国分部的联合创办人，并且积极参与硬件和电脑安全的研究工作。当他不和其他当地或国际的相关组织成员就安全事件进行合作时，可能会在中西部居住。作为一个传统的自学者，他拿到了来自新泽西 Ramapo 学院硕士学位。

Deviant Ollam 是一位网络工程师和安全顾问，最喜爱的工作是教书。作为一个从新泽西技术学院“科学、技术和社会”培训项目毕业的学生，他对研究人类的价值和科技世界的发展之间的相互作用非常入迷。他认为增加安全的最好的

办法是公开漏洞。他曾经在许多大学、会议发表这一见解，其中包括著名的西点军校。

Marc Weber Tobias, Esq. 是一位调查律师和物理安全专家。他曾经写了五本有关刑法、安全、通信的教科书。作为 Organized Crime Unit 的领导者，他曾经为司法部长办公室（Office of Attorney General）、南达科他州政府工作了好几年。Tobias 为许多执法部门做过演讲，同时还与许多国家的顾客和锁具制造商进行了交流。他的公司为特定的政府机构提供内部事件调查服务，也为私人客户提供国内调查服务。Tobias 主要为客户分析高级安全锁和安全系统的性能，并且参加了用来阻止攻击者进入的安全硬件的设计工作。他撰写了著名的《锁、保险柜和安全》（Locks, Safes, and Security），是执法部门必备的参考书。

序

每年我都会参加很多安全会议。我从未错过 Johnny Long 的演讲。Johnny 不仅是安全电路方面最风趣的演讲者之一，而且他的陈述充满了有趣的思想：在降低安全风险的过程中，基础才是最重要的。

Johnny 要求你不仅不能忽略周围最显眼的地方和还要对你周围的环境有更多的了解，他的非技术攻击呈现了一种称为 MacGyver 攻击的技术，这是一种以安全数据为前提的昂贵的安全技术。

企业每天花费上万美金在高技术安全防卫上，却没有关注简单的绕过技术，没有关注非技术黑客正在窃取他们的利益。本书中，Johnny 描写了安全专家应该考虑的可视攻击。在他们匆忙完成任务去解决下一个问题时，许多安全管理人员忽视了简单的缺陷，反而使得他们的复杂的技术形同虚设。

正当安全部门为自己的技术洋洋自得时，却忽视那些简单的威胁，而攻击者正式抓住这点占据了上风。入侵者将会采用攻击最薄弱的环节的方法，而许多看似完美的防护计划却一直在上演《碟中谍》（*Mission Impossible*）中的桥段。Johnny 将会让你很惊讶，他用手巾开锁，跟在一群职员的后面进入了一幢大楼；从垃圾中找出敏感的私人信息；用 Google 和 P2P 网络去挖掘内部职员和顾客之间传递的敏感信息；然后向你显示了所有的这些是怎样向攻击者敞开大门并攻击你的。

商业安全中最主要的因素是人的因素。如果攻击者打个电话给职员就知道防火墙已经关闭，或者能改变设置留一个后门，那么这些昂贵复杂技术将变得一无是处。社会工程学或许是攻击者最喜欢的方法。当你打几个电话就能够从那些没有防备的人那搜集到看上去无害的信息，而这些信息能让你畅通无阻时，为什么还要把时间浪费在某个精细技术的破解上呢？

在过去的生活中，作为一个黑帽黑客，社会工程学能让我创造记录，在几分钟便完成入侵。然后，我必须找到并发现技术的缺陷去达到我的目的。Jack Wiles 在本书中提供的社会工程学例子或许太完美了，显得不真实。不过，那仅仅是借

口——人的想象力可以想很多，很丰富。问题是，你和你的同事、职员，或者你的爸爸妈妈是否喜欢上了它？在《社会工程》这一章将深入介绍非技术攻击通常会运用哪些方法，而我们应该如何防范，并保护自己不受攻击。

本书中，无论普通读者抑或商业用户都将发现有价值的信息，这些信息将引起你的警觉。本书清楚地列举了那些经常忽略的威胁，在设计安全措施保护交易安全时，IT 管理人员应该充分考虑这些威胁。不仅专业读者会发现本书引人入胜，普通读者也将学到关保护自己信息安全的方法和知识，如身份窃取、入室行窃，以及通过电脑加固家庭防御系统等。与其前作 *Google Hacking* 类似，Johnny 再一次向我们呈现了一个有趣但也引人深思的攻击技术。

Kevin Mitnick

前言

什么是“非技术攻击”？

当我进入这个领域时，知道必须站在技术的前沿。我度过了许许多多不眠之夜，顺着我家的网线爬来爬去学习线路。我的实践很有成效，经过几年的努力，创立了一个小但精锐的试验团队。我非常好，很强壮。网络将在我面前倒下。我的同事都尊敬我，我想我是条汉子。然后我遇见了 Vince。

Vince，年纪 40 过半，鹰一般锐利的眼睛，有点像欧洲人，和公司里的那群人混在一起。他经常身着一件黑色皮革外套、一件漂亮的衬衣、黑色的休闲裤，偶尔会戴顶黑色的软呢帽，显得很有气质。他攻击的故事本身就是一个传奇。有人说他曾经是个联邦调查员，为政府的绝密工程工作，也有人说他是唯利是图的天才，把秘密卖给出价最高的人。

他很有才气，能够完成一些看似不可能的事情。他能够用神奇的电子传动装置开启锁，短路电子系统并获取信息。他曾给我展示了一套他创立的系统，叫做“van Eck”[1]。它可以发觉来自 CRT 显示器的电磁辐射，并重新整合，这样就能监视到 1/4 英里远的计算机的显示器。他告诉我一台黑白电视可能用来监听 900MHz 的手机谈话。至今，我仍清楚地记得在地下室用钳子把超高频调谐器和一台老黑白电视连接起来时的情形。当我从旧电视中听到了手机谈话时，就下定决心，要从 Vince 这学到一切能学得东西。

令人难以置信的是，我第一次干这工作是被迫的。幸运的是，我们有不同的任务。我的任务是内部评估，就是评估内部威胁。如果一个职员变成坏人，可能给网络带来无法形容的损害。为了完全评估这些，我们的客户提供工作间、网络接口和一个合法的非管理员用户名和密码。我的任务就是通过这些许可/权限去控

[1] http://en.wikipedia.org/wiki/Van_Eck_phreaking

制关键网络，实现管理。如果我们获得了储存在企业数据库内的秘密记录，我的努力就被认为是成功的。由于我的自信，我有一个接近完美的内部评估记录。

Vince 的任务是物理评估，就是仿效一个外部物理威胁。设备的物理安全特性是顶尖的。他们已经花了很多钱在这些昂贵的锁、传感器，以及监视传动装置上。我知道 Vince 将利用他技术使除去这些东西。我和他里应外合，整个工作就像灌篮一样轻松，我们就是“梦之队”。

当 Vince 让我帮助他评估物理部分时，我大吃一惊。我忽然想起一部 007 的电影，Vince 是“Q”，而我就是 James Bond，去攻击传动设备。Vince 提供装置，像 van Eck 之类的东西，而我渗透进去并暗中监视他们的监视器或其他一些东西。我一想到做这样的事情就想笑，电子键区系统和感应锁都不是我能干的活。当我从监视室的天花板上悄悄取下录像带时，我能想象到守卫的表情。

我迫不及待地想开始。我告诉 Vince 给我那些外国的机械装备，我将用它们去验证安全。当他告诉我没有带任何装置时，我认为他是在开玩笑。当他告诉我真的没有带任何工具时，我差点想把他推倒，但知道他是个黑带高手，因此我有礼貌地问他的想法。他说我们要去创造。真是个小气鬼，什么工具都不提供。我问他不用任何装置如何攻击一个高安全的大楼，他看了我一眼，咧嘴一笑。我决不会忘记那种笑。

我们花了一个早上检查，包括几撞建筑和一些职员停车场，周围都有保护栏。每个人通过前面的大门进出。幸运的是，大门是开的，没有人看守。Vince 开车进去，我们绕过一幢建筑，把车停在它后面，看了看那码头。

“那边”他说。

“哪里？”我问。

“那边”他重复道。

Vince 的幽默感有时很吸引人。当他给我废话时，我决不知道他说什么。我顺着他的手指，看到了一个码头。刚刚通过的大门，有些工人在搬着包裹。“码头？”我问。

“对，就是那里。”

我发出了“啐”的声音。

“正确，简单。”他说。

“我不是简单地说‘啐’，我说‘啐’的意思是那边有那么多人，而你却让我过去。”

“嗯，是的，”他说，“放松一点，就是看上去你好像在这里一样，跟他们问好，友善点，谈论一下天气。”

我照做了。慢慢地，我发现自己就是里面的人了。我在周围转了转，捡到了一些坦克的蓝图，像军用的东西，拷贝了一份，然后离开了。我估计我的心跳达

到了每分钟 400 次，并且开始想像军队监狱是什么样的，不知道关于 Bubba 的谣言是不是真的，但我认为是真的。这是一次难以置信的冲动。这是最简单的社会工程学实践，没一个人怀疑我。我想对他们而言这太尴尬了。当我走进汽车时，忍不住笑了出来。不过，我也没看到 Vince。几分钟后，他从楼里面出来，带着一小堆信纸。

“你是怎么进去的？”我问。

“和你一样。”

“为什么你自己不做呀？”我问。

“因为我开始不确定这样有用。”

我成了 Vince 的小白鼠了。不过没关系，虽然我全身发抖，但准备好了。我们的目标是下一幢楼，看上去像个堡垒。那没有码头，唯一的入口是前面的门。门是木头和钢铁做的（个人感觉很像城堡的门），大约 6 英寸厚，有个读卡器。我看到一个职员刷卡，拉开门正走进去。我建议我们跟着进去。Vince 摇头。显然他有其他计划。他走向大楼，当我们靠近前门时，他慢了下来。距门 6 英尺时，他停下来了。我走了一步超过了他，我回来头来，背对着门。

“天气很好呀，”他越过我看着门说。

“是啊，”我应付道。

“适合攀岩的好天呀。”

我开始转身看那楼。我可不想爬上去。

“别，”他说。“别转身，我们继续聊天。”

“聊天？”我问，“聊什么呀？”

“你看昨晚熊的游戏吗？”他问。我不知道关于他说的什么，也不知道熊是谁，不过他仍在继续说。“老兄，实际上不是那样的。团队的工作方式，它就像……”当前门打开时，Vince 停了下来。一个职员推开门，走向停车场。“他们是单独行动的，”他继续。我受不了了，我转身。门就已经关了。

“废话，”我说“我们可能已经进去了。”

“是啊，一个衣架。”

Vince 有时说些奇怪的东西。但那仅仅是冰山一角。他不是疯子，只是太部分人不能理解而已。我见证了他的狂人时刻。他说：“我们走，我需要一块毛巾。我必须回旅馆。”我不知道他为什么要一块毛巾，但我知道他还是个安全的狂人。我听说过斧头帮，还没听说过毛巾帮。

我们静静地回到旅馆；Vince 看上去仍沉迷在想法中。在旅馆前停下来后，他叫我等几分钟。几分钟后他出现了，拿着一个金属衣架和一块湿毛巾。他把这些东西放在车后面，然后说：“有它们就够了。”我不敢问。他继续说：“用这些东西我们可以进去了。”

我看了他一眼，也不知道我的表情是什么样子，但我觉得应该不会太好。我相信他要么是脑子进水了，要么是鬼上身了。我假装没去听他的，但他继续讲。

“每幢楼都有出口，”他说，“联邦法律规定，在紧急情况下，如果没有人知道出口门的操作方法，出口门必须从里面打开。”我眨了眨眼，通过挡风玻璃看天。我想知道外面的人是否会来接我。“此外，出口不需要钥匙和特别的代号。因此很容易通过出口门离开。”

我问：“我们是不是要对门做些处理。”这话让我十分惊讶。我已经开始跟着Vince 思路往下想了。

他看着我，我知道我看上去是什么样子。我本能地猛击可能在我头上的大蜘蛛。“这就是我们要对门要做的”他说，看着前面的窗口，靠左停下。我们又回到那个地方。他继续说：“那设备的前门很坚固，使用了重型磁性连接系统。我猜它可以抵挡一辆以每小时 40 英里速度行进的汽车的冲击。那些门很厚，可能是隐藏起来的，这系统非常昂贵。”

“但是你有毛巾，”我忍不住说。

“你注意到门上的出口装置没？”

我没有，我不可能说谎，于是承认道：“没有”。

“你必须留意任何东西，”他停下来看着我说，我点了点头。他继续说：“出口装置在一米多高的位置有一个银色的金属门闩。”

我照了下来。“哦，对，推动门闩。”这个词看上去还有点技术含量。

“不，那不是推动门闩。门闩是触摸的，不是压的。当它感觉到触摸时它就会进行操作，非常敏捷。”我们顺利解决了那地方的大门和停车场。Vince 解开扣子，从后座拿了衣架和毛巾。他拆开了衣架，拉成一跟长的直条。叠了一下，把毛巾放在尾端，沿着毛巾折衣架，把整个东西弯成了 90°的白毛巾旗，好像用来向保安投降，我当然不至于问这样愚蠢的问题。“我们走，”他说。

我们走向前门。大约下午 6：00，周围几乎没什么人。他走向那门，从门缝中挤进衣架的毛巾尾端，然后开始扭那衣架。我可以听到门另一边的毛巾的摩擦声。几秒钟后，我听到了一阵低沉的声音，Vince 拉开门，走了进去。我在一旁呆呆地看着，也没注意到门关上了。一会儿门又开了，Vince 伸出头。“你进来吗？”

这可以用以下文字描述：在花费数百万美元去保护他们的大楼后，他们认识到整个系统已经被一条毛巾和一个金属衣架打败了，所有这些都是因为没为门镀上仅仅价值 50 美元的门缝板。主管们表示怀疑，想要证据，这些证据不过是 Vince 走了一圈就得到了。我不知道在向公司演示结果时会发生什么，但是决不会忘记学到的经验：最简单的解决方案就是经常实践。

当然，我们可以破坏大楼的安全系统，先了解锁的磁性操作原理，或者测量墙的厚度，使用的焊条接在天花板上打一个洞，就像电影里一样。但我们不需要

那样。这就是非技术攻击的精髓。你需要掌握大量的技术知识，才能够取得和非技术攻击一样的效果，而这些技术却是没有重复性的。最糟的是，尽管很简单，一个非技术攻击或许是最致命的和最容易误解的。

这些年，我按照 Vince 的建议去学习。我现在注意一切东西，试着保持复杂的思维，几乎从来没有停下过。我经常看到新的攻击手法，而其中最危险的就是有可能被有攻击意愿的人使用的方法。

非技术攻击的关键

非技术攻击的关键就是简化思维、保持清醒、擦亮眼睛、昂起头。例如，当我去商场或其他人口密集的地方时，就会留意周围的人群。对我而言，陌生人是个有趣的难题，我会尽所能去获取有关他们的情况。当我在机场遇到一个商人时，头脑会加速运转，试着辨别他的座位号码和社会地位；了解他的医疗问题；探寻他的家庭情况（或他的性别取向）；推断他的收入水平和经济情况；推测他的饮食习惯；以及猜测他的家庭地址。当我去餐馆时，会观望周围进进出出的人，获取有趣的小道消息。分析周围环境时，我会全心身地沉溺于思考。当我走过停车场时，会留意两边的车辆，推断里面是什么，楼里的居民可能是谁。我做的这些事不是因为注意力集中，而是因为这是我的工作，一种习惯。我已经亲自见证了这种感知的威力。当面对非常棘手的安全挑战时，我不会指责谁。我停下来观察。提高感知能力的最好方法就是时时刻刻都在实战状态。

——Johnny Long

目录