TURING 图灵原创

黑客大揭秘

近源渗透测试

柴坤哲 杨芸菲 王永涛 杨卿◎著

中国工信出版集团 人民邮电出版社 POSTS & TELECOM PRESS

杨卿老师，在国内乃至世界黑客圈里，尤其在无线电安全研究领域，是一个颇具传奇经历和积极影响力的Hacker，同时又是一位有深刻情怀的网络安全科普专家，在国内网络安全人才急需的今天，这点尤其难得。所谓侠之大者，为国为民！希望此书的出版，能够引领更多网络安全技术爱好者，笃定自己的信念，取得更大的成就！

鲁 辉

中国网络空间安全人才教育联盟秘书长

网络安全人才是国家未来的希望，祝愿广大的网络安全爱好者能通过本书，修炼出属于自己的精湛技艺，为成为更优秀的自己而努力！

高杨扬

全国青少年阅读推广大使
中国少年儿童新闻出版总社首席品牌课程推荐官

我们读过很多关于网络安全的书，怎样入侵网站，怎样猜解密码，怎样用邮件钓鱼，大家都滚瓜烂熟。而这本书，讲述的是一种全新的攻击、全新的安全。黑客不再远隔千里，而是就在我们身边。他们就在公司楼下的咖啡馆，就在办公室门口，就在隔壁座位，等待一切可能的机会。

云 舒

默安科技联合创始人兼CTO

近源测试即利用各类无线网络、物理接口进行的渗透测试，往往是传统网络安全测试人员容易忽略的一条途径和技术盲点。本书作者均来自知名的无线安全研究团队PegasusTeam，有多年丰富的无线渗透测试经验。书中内容偏向实战，详细介绍了近源渗透中涉及的各种技术、工具以及示例，具有很强的可操作性。无论是作为入门材料，还是作为实际工作中的技术参考和扩充，这都是一本不容错过的好书。

陈雪斌（古河）

微软全球最具价值安全研究员Top1
国家杰出工程师青年奖获得者

本书作者具有丰富的物理渗透实战经验及多年无线安全研究经验。在远程攻击面较小或目标网络安全意识较高的情况下，近源物理渗透往往能达到“灯下黑”，出其不意地突破外层较为完善的防御，直达纵深。

anthrax@insight-labs

前Google高级安全研究员

本书作者们集网络安全的理论知识与实践经验撰写了此专著，在此表示祝贺！杨卿先生作为亚太体育联合会聘任的网络安全专家委员，肩负着融合与发展网络安全攻防技术与电子竞技运动的责任，任重道远。希望读者们通过此书习得网络安全真知，在磨练技术、提升水平的同时，在亚太体育联合会推广的网络安全电竞大赛上也能体现真我价值，为国争光！

曲正超

亚太体育联合会总会电子竞技运动委员会秘书长

杨卿作为国内名列前茅的无线通信和IoT（物联网）安全专家，一直走在国内安全科普的第一线。我相信本书的出版，一定能为安全圈带来更多的新鲜血液，本书也将成为近源渗透领域的启蒙之作！

谢 忱

斗象科技CEO
FreeBuf联合创始人

认识本书作者团队很多年了，他们一直专注于无线电通信安全的研究，在该领域有着丰富的实战经验和技术积累。此书将向读者们揭露来自真实世界的无线攻防，以近源渗透的角度展示如何绕过和打破企业想象中完善的安全防护体系，直抵内部关键系统。相信此书能启发国内安全行业对近源渗透领域的关注。

sunwear

知名网络安全、信息网络战专家

近年来，黑客的攻击已不再局限于远程的网络入侵，企业的各类无线网络、物理接口开始成为黑客新的攻击入侵途径，进而形成了近源渗透一整套创新的攻击方式，安全人员结合运用社会工程学和近源渗透往往能够取得非常好的效果。安全从业者通过本书的学习，可以拓宽自己的思路，更好地理解近源渗透的攻击技术，提升企业的安全防护能力。

宋申雷（rayh4c）

360高级威胁应对团队安全专家

封面插画设计：赵萌曦

图灵社区：iTuring.cn
热线：(010)51095183转600
分类建议 计算机 / 网络安全
人民邮电出版社网址：www.ptpress.com.cn

TURING 图灵原创

黑客大揭秘

近源渗透测试

柴坤哲 杨芸菲 王永涛 杨卿◎著

人民邮电出版社
北 京

图书在版编目（CIP）数据

黑客大揭秘 : 近源渗透测试 / 柴坤哲等著. -- 北京 : 人民邮电出版社, 2020.1
（图灵原创）
ISBN 978-7-115-52435-5

Ⅰ. ①黑… Ⅱ. ①柴… Ⅲ. ①黑客－网络防御 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2019)第239928号

内 容 提 要

本书主要讲解了当渗透测试人员靠近或位于目标建筑内部，如何利用各类无线网络、物理接口、智能设备的安全缺陷进行近源渗透测试。书中首先以 Wi-Fi 举例，介绍基于无线网络的安全攻防技术及实例测试，包含对家庭、企业级无线环境的常见渗透测试方法，无线入侵防御解决方案，无线钓鱼实战，以及基于无线特性的高级攻击利用技术；然后介绍了当渗透测试人员突破边界后可使用的各类内网渗透测试技巧，如敏感信息收集、权限维持、横向渗透、鱼叉攻击、水坑攻击、漏洞利用、密码破解等。此外，我们还介绍了针对门禁系统的 RFID 安全检测技术、针对 USB 接口的 HID 攻击和键盘记录器技术、网络分流器等物理安全测试方法。

无论是信息安全爱好者、相关专业学生还是安全从业者都可以通过阅读本书来学习近源渗透测试的相关技术并扩展安全视野。本书并不要求读者具备无线安全及渗透测试等相关背景，仅需掌握基础的计算机原理即可。当然，拥有相关经验对理解本书内容会更有帮助。

◆ 著　　柴坤哲　杨芸菲　王永涛　杨　卿
责任编辑　王军花
责任印制　周昇亮
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京市艺辉印刷有限公司印刷
◆ 开本：800×1000　1/16
印张：21.75
字数：502千字　　2020年 1 月第 1 版
印数：1－3 500册　　2020年 1 月北京第 1 次印刷

定价：99.00元

读者服务热线：(010)51095183转600　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

序一

独角兽安全团队在 2016 年出版了国内无线电安全领域的著作《无线电安全攻防大揭秘》，其中包含了从近距离的 RFID 到远距离的卫星通信等各种无线技术的安全漏洞及攻防案例。不过在那本书中缺少了非常重要的一项无线技术：Wi-Fi。这是因为 Wi-Fi 安全涉及的内容非常多，当时我们觉得应该为 Wi-Fi 安全单独出一本书，现在，这本书终于面世了。

实际上，整个无线安全领域开始受到公众广泛关注，其中很重要的原因便是 Wi-Fi 安全领域的发展与各类 Wi-Fi 安全事件的曝光。Kali、大菠萝等普及率很高的攻防软件和硬件工具的出现，使得 Wi-Fi 攻击技术逐渐变得低门槛化、低成本化。目前，Wi-Fi 作为在家庭和企业环境中拥有非常高覆盖率的无线接入技术，已经成为 IoT 时代智能设备的首选无线协议，因此 Wi-Fi 存在的安全问题会影响到大量的智能设备，甚至威胁到设备所连接的企业网络，最终导致内网渗透。我想这便是“近源渗透测试”概念提出的缘由。

这可以说是国内少有的以红队（Red Team）为导向的近源渗透测试及内网渗透的书。本书不像以往类似题材的书，只是对加密算法和基础无线破解的泛泛而谈，而是结合天马安全团队多年在渗透测试服务中汲取的精华编撰而成。我相信，通过实践与理论的结合，能帮助读者们更透彻地理解并掌握近源渗透测试的相关技术。

黄琳

360 安全研究院技术总监，独角兽安全团队负责人

序二

首先感谢王永涛（Sanr）邀请我为此书作序，第一次看到书稿大纲时确实很意外，因为这将是国内甚至国际“近源渗透”领域少有的成体系的中文书。Sanr 所在的天马安全团队（PegasusTeam）在无线安全领域有着非常丰富的实战经验，除此之外，Sanr 在内网渗透方面也有很深的沉淀。所以当收到他的邀请时，我对此书是充满期待的。

近源渗透需要在物理上接近目标，对社会工程学方面的能力要求相对更高。从实战意义来说，近源渗透的价值是被大大低估的，这有一个很大的原因：企业在网络安全建设环节，对于云安全、外网安全等这些偏向外部威胁的安全建设一般会落实得比较到位，但内网安全、物理安全、人员安全这些偏向于内部威胁的安全建设往往会是比较大的薄弱点。许多企业会觉得“近源攻击”是电影情节，极少在实际运作中遭遇。但我的观点不一样，随着这两年红队（Red Team）理念的风靡，许多大型企业都开始构建自己的红蓝对抗。这里的大背景是全球黑客威胁的纵深化，比如洛克希德·马丁描绘的 APT 七步杀：情报调研、武器化、分发、利用、植入、C2 控制、进一步行动。这里的“进一步行动”还可以继续细分，比如持久化、横向移动等。七步杀的“分发”除了远程攻击，还有一种就是“近源渗透”，比如通过 Wi-Fi、USB、蓝牙、NFC、RFID 等进行攻击。这些内容在此书中会有系统性讲解，这是我觉得很赞的。

熟悉我的人应该知道，我比较擅长前端黑客领域，在这个领域也出过一本书。但过去几年，我在网络空间安全攻防上也有了不少沉淀，为大家所知的是我带队打造的 ZoomEye（钟馗之眼）网络空间搜索引擎，而过去两年我组建了自己的红队 Joinsec，开始在渗透领域进一步实践相关攻防点。我的这些经历让我对此书的面世更有感觉，这本书会成为这个领域的经典。

余弦

慢雾科技联合创始人，《Web 前端黑客技术揭秘》作者

前言

10年前，国内网络安全圈的黑客们还专注于最初级的无线网络安全研究，采用最传统的无线攻击方法破解 Wi-Fi 密码、蹭网，继而进行网络渗透测试。那个时期也是无线局域网安全最火热的时期。无线网络安全研究者们专注于寻找性能更优良的无线网卡，搭配着自己优化的无线破解平台或直接使用 BackTrack、BackBox 以及后来的 Kali、NetHunter 等完善环境来对身边一个又一个无线热点进行安全评估，体会那种突破限制、接入目标网络的成就感，同时也完成了对于企业安全评估的“红蓝对抗”。

随着无线攻防对抗的不断迭代，许多更有趣的攻击方式也出现了。例如 EvilAP 钓鱼攻击：先侦测由无线客户端主动发出的 Probe 帧中泄露的“历史连接热点名称”，通过软 AP 程序（hostapd）创建同名的钓鱼热点，将无线目标拉入虚假的无线环境，进而发起攻击或窃取目标网络流量中的敏感信息。

2015 年 3 · 15 晚会上，由独角兽安全团队支持的 Wi-Fi 安全环节让圈里的资深无线网络安全研究者们为之动容。这个演示环节的灵感来源于 DEFCON 黑客大会 Wireless Village 上有名的绵羊墙（The Wall of Sheep）。绵羊墙将收集的账号和隐匿的密码投影在影幕上，告诉人们：“你很可能随时都被监视。”

随着时代的发展，各类无线通信技术也出现在了各类政企单位的基础设施中。这里列举一个早年间存在于北京某条地铁线路的安全问题。我们知道，高速行驶的地铁列车需要将车厢内的广告系统、视频监控、列车运转状态等信息实时回传到站台，以便站台对列车的整体状态进行把控。那么问题来了，数据该如何有效回传呢？列车不可能在行驶过程中还拖着传输线缆，此时就需要用到无线通信技术。在当时的科技背景下，多数会选择 2.4 GHz 频段的无线局域网通信方案，但是后来出现了大家所熟知的 WEP 安全缺陷，以及针对 WPA 和 WPS 的各种在线、离线与云端集群密码破解的诸多方法，甚至是利用“Wi-Fi 热点万能连接器”App 从云端提取已被分享的 Wi-Fi 连接密码，这些威胁最终都会导致无线网络被攻击者轻易破解，并将私有设备接入地铁运行网络，继而引发更深层次的渗透测试。因此，在选择无线连接方案时，务必要经过严谨且有效的安全评估，而一旦在基础设施上出现安全问题，后期再进行升级修复的成本就非常高。安全人员一定要抱有这样未雨绸缪的思维来看待无线安全建设的重要性。

从另一方面来看，无线通信上的漏洞给予了攻击者以非接触方式对目标系统发起攻击的机会。事实上，截至目前，无线通信安全依然是政企单位在规划整体安全方案时常被忽略的一点。几年来，天

马安全团队（PegasusTeam）在获得渗透测试授权的情况下，利用各类无线网络对军工、能源、金融、政企、基础设施的网络进行了测试，都取得了 100% 的渗透测试成功率，这足以说明我们对无线网络安全的建设与防护依然处于相对模糊且薄弱的阶段。

我们把这类利用无线网络进行渗透测试的方法命名为“近源渗透测试”。在传统的网络测试中，各类防火墙、入侵检测等防护产品已经较为成熟，攻击者很难通过外网的网络入口突破企业的重重防御。而在近源渗透测试的场景中，攻击者位于目标企业附近甚至建筑内部，这些地方往往存在大量被忽视的安全盲点。结合近源渗透的相关测试方法和技巧，攻击者可以轻易突破安全防线进入企业内网，威胁企业关键系统及敏感业务的信息安全。

本书整理了我们在进行近源渗透测试时使用的从突破边界到内网渗透的种种技术。近源渗透测试和普通的渗透测试在“边界”概念上存在很大的区别，从现状来看，前者的突破口大多还是以 Wi-Fi 为切入点的。不管是通过现场破解无线密码，还是通过云端的集群破解密码，攻击者只要拿到了正确的凭据，便可以进入目标网络。当然，我们在对外进行渗透测试的时候，很少使用这种“硬碰硬”的方法。思路是活的，通过前期“踩点”的结果可以或多或少发现，这个企业中一定存在员工私建的或不知道什么原因建立的临时热点，这些热点都可以合理跳过 ACL（access control list，访问控制列表）的限制，为我们进行深层次渗透测试提供便利条件。

后来在多次渗透测试的时候，我们思考了一个问题：渗透测试人员是不是必须抵达目标附近？受电影 *Who Am I* 的启发，我们突然有了灵感，使用树莓派 Zero，通过 3D 打印机制作了一个外壳并搭配大容量的移动电源。在踩点时拿到了用户的无线接入凭据，将树莓派接入无线网络，反向回连到云主机并将设备留在现场，随后渗透测试人员在家中便可远程进行后续工作了。后来我们还使用 Arduino 做了一个小硬件，它可以达到 12 小时的续航，在遇到不能及时完成的渗透测试工作或者需要远程协助的情况下，它可以起到“跳板机”的作用。

通过这些年的实践，我们发现近源渗透测试本身就是一个多样化的渗透测试行为，我们可以根据目标的网络状态、现场环境、物理位置等因素灵活地更换渗透测试方式，这也更接近渗透测试的本质。当然，我们也设想过在更加智能化的将来，企业可能会使用更先进、更智能的设备，如摄像头、饮水机、扫地机、门禁、虹膜系统等，它们可能配置有更先进的无线传输协议，这些协议是否也存在安全漏洞呢？答案是肯定的。到那个时候，《碟中谍》系列电影中的各类攻击场景，将不仅仅是只存在于电影中的臆想了。

我相信，我们肯定不是第一个从事“近源渗透”的团队。通过本书，我们想把经验分享给更多安全从业者，不管是蓝军还是信息安全团队，希望你们都能通过本书受到启发：安全永远需要未雨绸缪，因为你不知道什么时候，你所在的公司楼下就有一帮想黑掉你们的坏家伙。

本书内容共分为 7 章及附录。

- 第 1 章介绍我们对近源渗透测试的思路、理念以及对该领域未来的展望。
- 第 2 章以 Wi-Fi 为例，介绍基于无线网络的安全攻防及实例测试，包含家庭、企业级无线环境的常见渗透测试方法，无线入侵防御解决方案，无线钓鱼实战，以及基于无线特性的高级攻击利用技术。
- 第 3~7 章介绍渗透测试人员突破边界后可使用的各类内网渗透测试技巧，如敏感信息收集、权限维持、横向渗透、鱼叉攻击、水坑攻击、漏洞利用、密码破解等。其中第 6 章还介绍了针对门禁系统的 RFID 安全检测技术、针对 USB 接口的 HID 攻击和键盘记录器技术、网络分流器等物理安全测试方法。
- 附录介绍了常见的近源渗透测试设备，并分享了两个真实的近源渗透测试案例。

为了保证描述准确、便于读者理解，书中部分技术术语直接使用英文，并在括号里面注明中文。文中提到的工具、链接及相关代码等，可以访问本书在 GitHub 上的项目主页获取：https://github.com/PegasusLab/near-source-pentesting-notebook。

《中华人民共和国网络安全法》已于 2017 年 6 月 1 日正式实施，不仅对网络运营者提出了要求，也对网络安全从业者提出了要求。现在普遍的“白帽子”渗透测试行为其实存在着较大的操作过失风险，现将需要大家特别关注的要点进行整理。

(1) 在进行渗透测试前需要取得客户授权。
(2) 请在客户授权的范围和时间内进行测试。
(3) 发现漏洞应尽快通知用户，不向任何第三方公布或传播漏洞。
(4) 不窃取、出售、篡改用户的敏感数据。
(5) 不恶意攻击服务器，不在服务器中留“后门”。
(6) 不对国家关键基础设施系统实施渗透或干扰行为。
(7) 不协助他人恶意攻击服务器，不提供或传播恶意攻击程序。

知其攻，后知其防。攻防对抗是信息安全研究健康发展的必然形式，但请各位读者务必要遵守相关法律法规，不得出于任何非法目的而使用本书提到的技术。如您因此触犯法律，我们对此不承担任何法律责任。

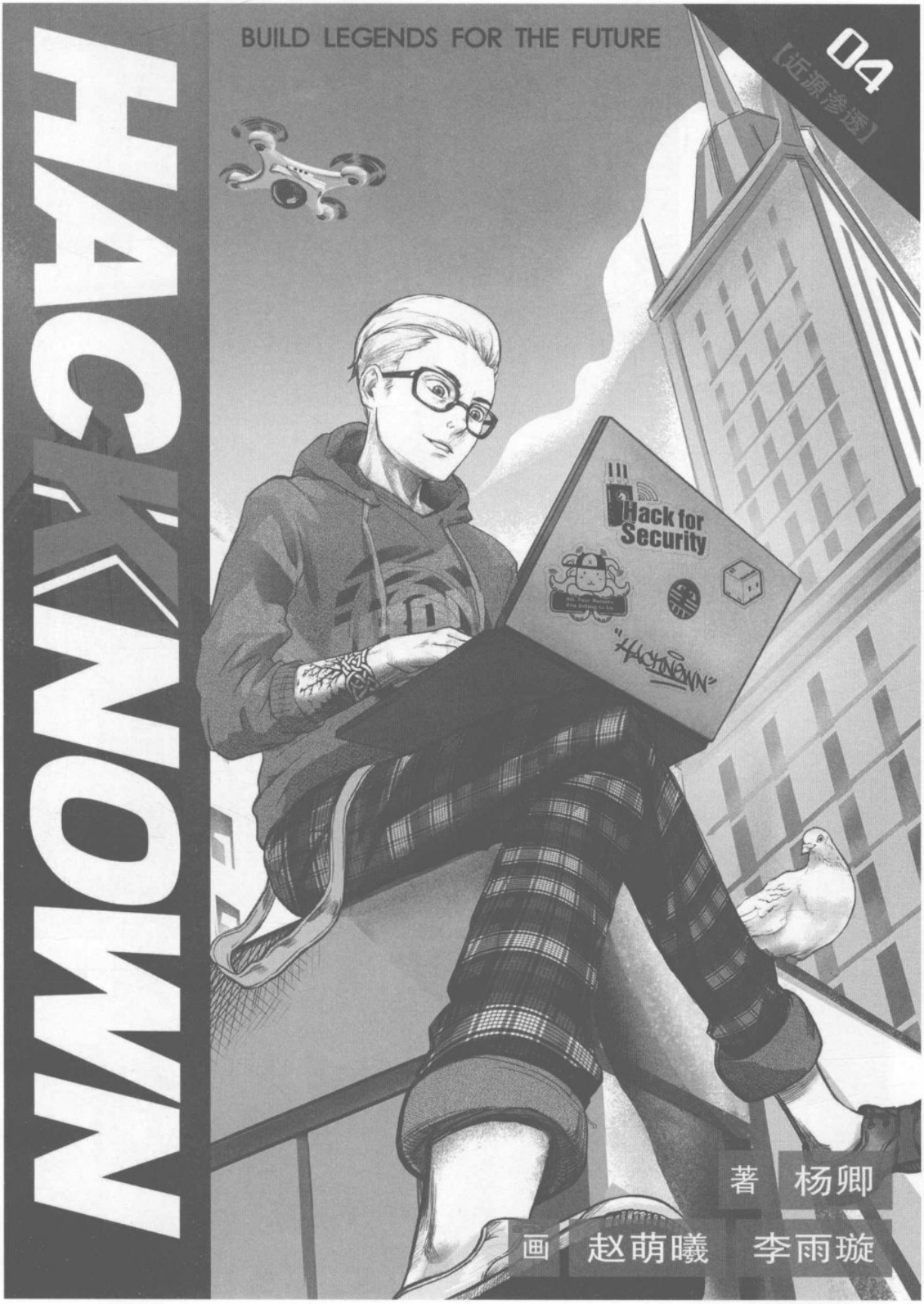
在本书开始前，我们摘录来自 360 黑客安全研究院的黑客漫画《黑客特战队》中的“第 4 话 近源渗透”内容作为预热，希望读者朋友们可以从中感受到近源渗透测试的魅力！

HACKNOWN

BUILD LEGENDS FOR THE FUTURE

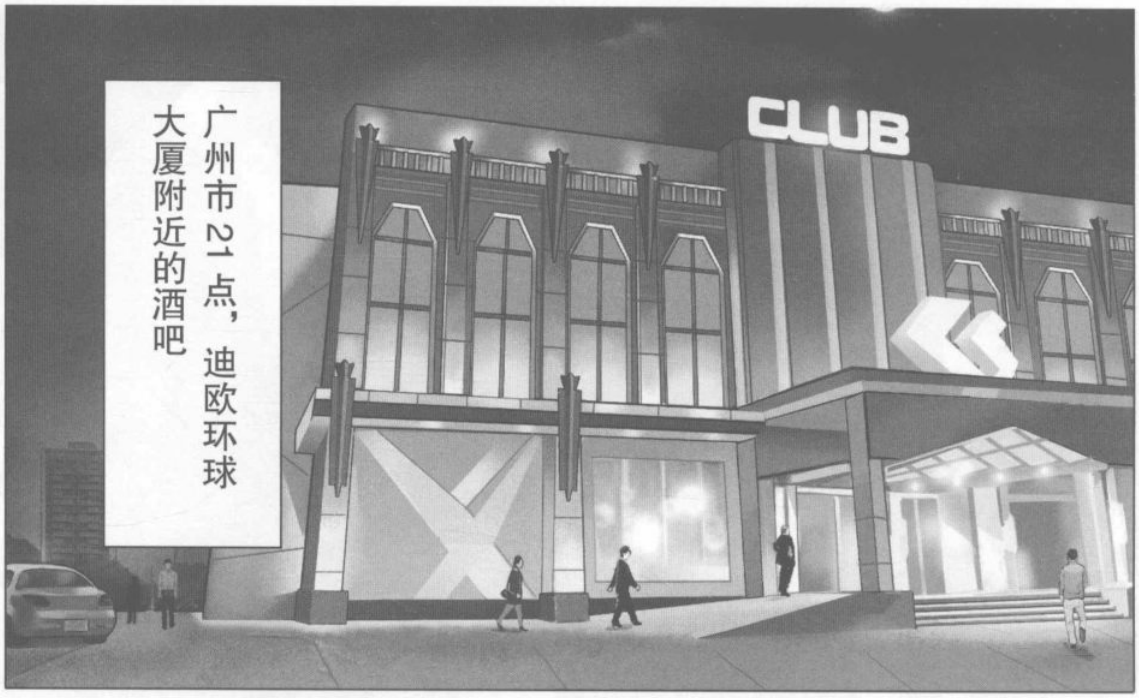
04

【近源渗透】



著 杨卿

画 赵萌曦 李雨璇



广州市21点，迪欧环球大厦附近的酒吧

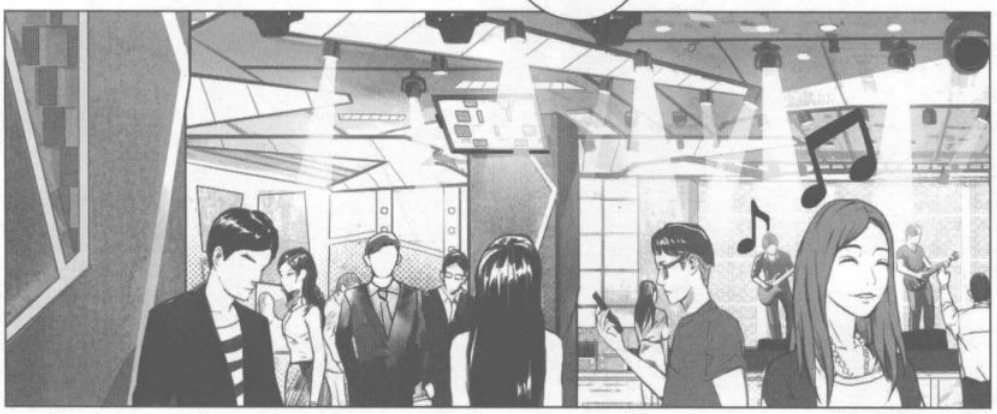
众所周知，人类自然寿命是全球平均寿命的1到1.5倍。但疾病就像一把加密锁，牢牢地锁住我们生命界限的大门。我们迪欧生物制药集团所研制的儿童疫苗，就像一层牢不可破的健康护盾终身保护伴随着你。抵御各种医学界都难以控制的传染病，实验安全率达到100%。我们的座右铭是：一支疫苗终身受益，健康造福你我他！

哼！这个道貌岸然的家伙。

不要以为生产无效疫苗坑害了孩子们还能逍遥法外，不了了之！


Christian Dio
迪欧生物制药科技有限公司
杜刚
首席技术官
Christian Dior Biological Pharmaceutical Co., Ltd.


情报说这个杜刚是迪欧的高层管理人员，具有很高的权限，每天都会来这里喝几杯。

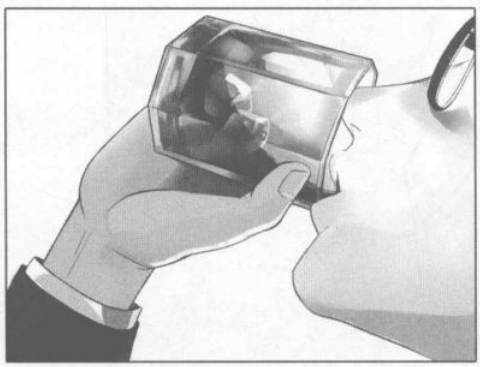


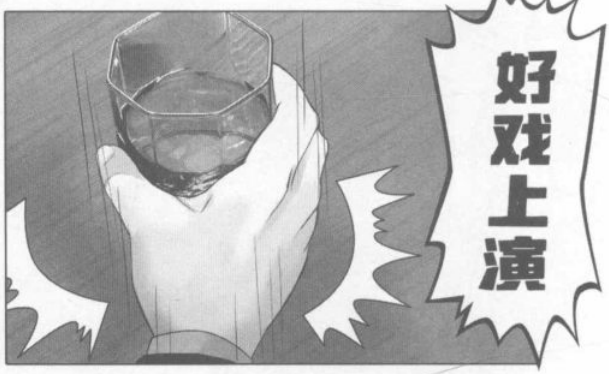

你知道吗，我要开始正义审判了！等着为我喝彩吧，扮演英雄的故事即将开幕！


来了


STAFF D CARD
BANG DU


听说迪欧集团的新型疫苗就是由杜老板的技术组研制开发出来的呢，看来杜老板升职加薪指日可待了呢。
杜老板！你在迪欧的职位很高吧！




好戏上演


喝什么，我买单。
杜哥，你真是越来越帅了啊！
是呀，是呀。
“发动”HACKING
拍
“RFID SECURITY”
喂！你干什么？有病呀！你知道我是谁吗？
笑


第二天早晨
迪欧大厦
通过门禁卡秘密潜入迪欧大厦的档案数据中心，揭露你们真正的实验数据。


嘈杂声
掏
先生！请您将金属物品取出来，U盘、移动硬盘等一切存储设备都不能带入办公楼。