前言

我第一次遇见凯文•米特尼克是在 2001 年，那时探索频道正在拍摄记录片《黑客的历史，不为人知的地带》。两年后，我飞往匹兹堡参加了他在卡内基-梅隆大学的演讲会，在那儿我听完他的黑客故事后惊呆了。他闯入企业的电脑，却不破坏任何文件，获得了很多信用卡号码，既不拿来用也不卖掉，他搞到了一些软件（源码），却一直放在“口袋”里。他的黑客行为只是为了好玩，只是为了挑战。 在他的演讲里，凯文详细的描述了他是如何化解 FBI 对他的抓捕行动的。凯文入侵了 FBI 的管理系统，从而得知了整个行动计划，还发现有一个新认识的黑客“朋友”一直在做 FBI 的线人，不仅得到了该 FBI 小组所有成员的名字和家庭地址，甚至还监听了那些想要搜集证据抓他的人的电话和语音信箱。为此他建立了一个预警系统，可以在 FBI 准备行动之前提前通知他。

电视制片人在放屏保的间隙邀请凯文和我参加他的一个节目，他们要我展示一下一个刚进入市场的新设备：GPS（全球定位系统）。我本来应该开车转悠一下，好让他们追踪我的车，可在天上，他们看到的随意的驾驶路线却组成了一句话：

释放凯文（FREE KEVIN）

我们再一次分享麦克风是在 2006 年，当时凯文做客阿特·贝尔的访谈节目“从大西洋到太平洋”，他邀请我作为特殊来宾参与节目，然后我听到了很多关于他的故事，那天晚上他采访了一些我的事，我们度过了一段欢乐的时光，那感觉就像是我们经常这样做一样。

我的生活已经被凯文改变了，有一天，我发现他的电话都是从很远的地方打来的：有时是在俄罗斯演讲，有时是在西班牙帮助一家公司维护信息安全，或者是在智利给一家银行提关于计算机入侵的建议，这听起来很酷。我已经有大约 10 年没使用过我的护照了，直到这些电话把我的心挠得痒痒的。凯文让我和出版他演讲的代理商联系，她告诉我，“我也可以去为你演讲。”所以感谢凯文，我已经成为了一个像他那样的国际游客。 凯文已经成为我最好的朋友之一，我喜欢待在他的身边，听那些入侵和冒险的故事，他的生活就像是最佳影片一样扣人心弦。

现在你可以读到所有这些故事，这些年我听到的一段又一段紧张而又刺激的冒险。在某种程度上，我很羡慕读者们即将开始的这段旅程，进入到凯文•米特尼克那些难以置信的故事和传说中。

- 史蒂夫·沃兹尼亚克
苹果公司联合创始人

序章

从“物理入口”溜进目标公司的建筑从来都不是我喜欢做的事。这种方法太冒险，连把它写下来都让我出了一身冷汗。

我是这样做的，在暖暖的春季傍晚，我悄悄地躲在一个昏暗的停车场里，旁边就是一家市值上亿美元的企业，我静静地等待着时机。一个星期以前，我就已经在白天去过这栋建筑了，使用的借口是寄给该公司员工的一封信丢失了，这给了我机会仔细查看他们的身份卡（ID cards）。这家公司把雇员的头像放在证件的左上角，名字在下面，姓在前名在后，使用了印刷体大写字母，公司名称在卡的底部，是红色的，当然也是用的印刷体。

我跑到金考快印，从那家公司的网站把他们的 logo 下载下来，粘上我自己的照片扫描件，然后花了大约 20 分钟的时间用 Photoshop 修改，就打印出了一个可信度很高的公司 ID 证件，我还把它在一角钱商店过了塑。然后我为一个朋友制作了另一个假证件，他要跟我一起进去。

插播一条快讯：假证件甚至不需要多高的仿真度，百分之九十九的的时间它只会被匆匆瞟上一眼，只要基本信息是在正确的地方，看上去像是那么个样子，你就能混过去，当然，一些过度热心的警卫或员工会极为敬业的把它拿近了看。不过如果你像我一样过日子，这就是必须面对的风险。

我藏在停车场，看着那些烟瘾上来了的人跑这里吞云吐雾，我等啊等，总算等到一小撮大概五六个人开始返回大楼。后面的门可以用员工的门禁卡解锁，大家都排着队通过那张门，我也跟着溜在了后面，我前面那个人进门的时候发现后面还有一个，他瞥了一眼我的胸牌，帮我把门卡住了。我点头表示感谢。

这种技术叫“尾随”。

在里面，我第一眼看到的是一个标志，你进门马上就会看到。那是一个安全告示，警告不要为任何人卡门，要每个人用自己的门禁卡解锁。但出于公共礼节，很绅士的“资深员工”经常会忽视这些安全警告。

大楼里，我开始四处漫游，这是一项重要任务，事实上我是在找信息技术（IT）部门，大约十分钟后，在大楼的西侧我找到了这个地方。我之前做足了功课，弄到了这家公司一个网络工程师的名字，我估计他可能有这家公司完整的管理员权限。

该死！当我找到他的工作室时，发现这不是一个容易进去的地方，一个单独的办公室……一张锁着的门。还好我找到了一个解决方案，天花板是用那些白色的隔音板做的，这种东西经常被用来做空间较狭小的吊顶、各种管道和电气线路等等。

我用手机打电话给我那个朋友，说我需要他，然后我回到后门带他进来，这是个瘦高个儿，我希望他能做点我做不到的事。回到 IT 部门，他爬上一张桌子，我再抓住他的腿搭成人梯，这样他就能把天花板的格子顶起来，然后我脚尖一踮，他一把抓住上面的管道爬了上去。不到一分钟，我就听到他掉进了里面那间上了锁的办公室。门把手一动，他笑嘻嘻的站在那里，带着一身的灰。

我走进去悄悄地关上门，我们现在安全了，不大可能被人发现。办公室很黑，把灯打开很危险并且没有必要，从工程师的计算机上发出的亮光已经够让

我看清任何东西了。我快速的查看了一下他的桌子和抽屉，还有键盘底下，看他有没有留下写有他密码的纸条。不走运，但没关系。

我从腰包里掏出一张 CD，上面有可启动的 Linux 操作系统和一个黑客工具包，放进他的 CD 驱动器里然后重启电脑。其中的一个工具可以让我改变他电脑上的本地管理员(Administrator)密码，我把它改成我想要的，然后我拿掉 CD 再重启电脑，这一次我就可以用本地管理员帐号登录了。

我以最快的速度安装了一个“远程访问木马”，这种恶意软件可以让我完全控制这台机器，可以记录键盘输入、截取哈希密码，甚至可以用摄像头拍下使用这台电脑的人的照片。我安装的这个木马会通过互联网每隔几分钟就主动连接（反弹木马）在我控制之下的另一台电脑，让我获得目标系统的控制权限。这就差不多完成了，最后一步，我进入注册表把“最后登录的用户”设定为那个工程师的用户名，这样就不会有任何证据我用本地管理员帐户登录过。那个工程师上班的时候会发现他已经注销登陆了，没关系：只要他再登录进去，一切就和往常一样。

我准备走了，我的伙计已经“修”好了天花板，在出去的时候顺便把门给锁上。

第二天早晨，工程师在大概8点30分的时候回到他的电脑旁，与我的笔记本电脑建立的连接，因为木马的缘故，我有了完整的域管理员权限，然后我只花了几分钟的时间调出包含整个公司所有帐号密码的域控制器。一个叫做“fgdump”的黑客工具可以让我下载所有用户哈希过（Hashed）的密码。

几个小时后以后，我便通过“彩虹表”——一个巨大的预先计算好的哈希密码数据库——破解了这家公司绝大多数员工的密码。最终我找到了一台处理客户交易过程的后端计算机服务器，但发现信用卡号码是加密过的。没关系：我发现加密卡号的密匙就藏在数据库的存储过程中，大家都知道“SQL 服务器”是可以被任何数据库管理员访问的。上百万的信用卡号码我可以用这些信用卡没日没夜的买东西，每次都用不同的卡买，怎么买也用不完。

但我没有这么做，这个真实的故事并不是那些会让我进局子的入侵回放，这实际上是有人花钱请我做的。 我们把它称之为“渗透测试（pen test）”，“penetration test”的简称，这已经成为了这些天我生活的一大部分。我已经入侵了一些地球上最大的公司，渗透进那些超强悍的计算机系统里——这些公司花钱请我这么做，帮助他们修复漏洞，改善他们的安全状况，这样他们就不会成为下一个入侵受害者。我主要是自学成才，并已经花了数年的时间去研究攻破安全系统的方法、战术和战略，还学习了很多关于计算机系统和通信系统的底层内容。

对于技术的热情让我走过了无数坎坷的道路，我的黑客恶作剧让我在监狱里浪费了超过五年的时间，并给爱我的人造成了巨大的心理创伤。

这是我的故事，所有的细节都是准确的，包括我的记忆、个人笔记、公共法庭记录、包还有真实自由信息的文档、FBI 的窃听和贴身录音、很多小说的采访和两个政府线人之间的讨论。

这是我如何成为世界头号通缉黑客的故事。