聚焦黑客

——攻击手段与防护策略

张耀疆 编著

人民邮电出版社

图书在版编目(CIP)数据

聚焦黑客——攻击手段与防护策略 / 张耀疆编著. —北京：人民邮电出版社，2002.9
ISBN 7-115-10516-2

I 聚… II. 张… 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(2002)第 056565 号

内 容 提 要

本书从网络安全所涉及的攻击和防御正反两个方面入手，在深入剖析各种黑客攻击手段的基础上，对相应的防御对策进行了系统的阐述。本书以黑客攻击计算机网络时所惯用的手段作为主线，全书分为 6 章，每个章节详尽地阐述了该阶段所特有的各种攻防技术，最后从维护网络系统安全性的全局考虑，详细讲解了网络安全建设可采用的整体解决方案。

本书最大的特点就是可操作性强，无论是攻击还是防御技术，除了介绍必要的基础知识并深入分析其原理外，还介绍了典型工具及操作实例，力求让读者在攻防技术的实际运用中建立起对网络安全深刻的认识。

本书适合从事网络系统管理的专业技术人员阅读，也可供对网络安全技术感兴趣的读者参考。

聚焦黑客——攻击手段与防护策略

◆ 编　　著　张耀疆
责任编辑　马　嘉

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress com cn
网址　http://www ptpress com cn
读者热线　010 67180876
北京仪魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：37 25
字数：913 千字　　2002 年 9 月第 1 版
印数：1 5 000 册　　2002 年 9 月北京第 1 次印刷

ISBN 7-115-10516-2/TP・3014

定价：48 00 元

序

目前，国内已经出版了不少网络安全方面的书籍，但鲜有介绍攻击技术内幕的优秀书籍，少数几本不错的资料也都是国外畅销书的中译本，我们非常希望看到能够代表国内安全水平的资料出现。这本《聚焦黑客——攻击手段与防护策略》令我们眼前一亮。虽然以专业的角度审阅此书，还能提出不少可以商榷的问题，但作者在本书中，对黑客攻击和防范技术做了精心的收集和系统的整理，体现出相当专业的水准。

一次成功的攻击，取决于攻击者的动机（自我挑战、报复情绪和利益驱使）、机会（找到各种可以利用的漏洞）和能力（攻击技能）三方面的条件；作为安全防御者，你需要做的就是削弱攻击者的动机（加强管理，使用威慑力量，如法律），杜绝受攻击的可能性（使用必要的安全技术、弥补技术和管理上的漏洞等）以及掌握比攻击者更强的技能（做到知己知彼）。

本书适合各企业的安全管理员，系统维护员，安全专业人士和计算机安全爱好者阅读。通过对本书的研读和实际操作，了解攻击原理，利用攻击的手段测试系统的安全性，并进行相应的安全加固配置，这是系统维护和管理人员需要掌握的一项重要技能。

本书并未就某类技术问题作深入的探讨，而是系统地阐述了现今流行的攻击手法，依据常见的攻击过程，对人们讳莫如深的黑客攻击方法进行了全面的阐述。作为专业人士的参考资料和操作指南，本书在以下几个方面是具有特色的：

- 书中总结了大量的经典攻击方法与测试工具，例如 Nmap、NC、Rootkit、Sniffer 系列等。
- 介绍了许多业界著名的商业安全产品或常用安全防护工具，如 ISS 系列、SolarWinds、PortSentry、Snort、SSL、PGP 等。
- 结合了国内的一些实际情况和特有的工具，如天网个人防火墙、小榕系列软件、冰河、Xscan 等。
- 分析了一些最新的安全问题和攻击方法，如交换网络监听问题、Unicode 问题、邮件与浏览器安全问题、IIS 问题及 Nimda、CodeRed 等蠕虫问题等。
- 在全书各个部分穿插和总结了与安全相关的基础背景知识，如 SMTP、Proxy、FTP、TCP/IP 协议族等。
- 书中详细列举了安全建议、安全配置方法，如 Windows 2000、UNIX 的安全配置和管理等。
- 提供了丰富的安全参考文献和相关的站点链接。
- 本书同样也关注到了安全管理的方法和标准，如 BS7799 等。

我们非常高兴能向社会推荐《聚焦黑客——攻击手段与防护策略》这样优秀的安全教材，也希望通过此种办法将我们的信息安全知识管理与教育服务体系延伸到广大读者中，通过各

种途径向读者传播最先进的安全技术和理念，为中国的信息安全事业做出贡献。我们非常乐意为国内优秀的信息安全作品提供鼓励和帮助，同时希望有更多的有识之士加入到信息安全领域，为构筑中国的信息安全事业共同努力。

安氏互联网安全系统（中国）有限公司

Information Security One（China）Ltd.

2002 年 8 月

注：安氏公司是国内最大的信息安全服务与解决方案提供商，汇集了国内顶尖的安全专业技术人员，在安全业界具有很高的声望。

前　言

美国《金融时报》报道，平均每 20 秒这个世界就发生一起黑客入侵互联网的事件；美国国际数据公司（IDC）2002 年 3 月 8 日宣布，全球大约四分之一的互联网应用服务提供商（ASP）的网络安全和病毒防护措施达不到标准；2002 年最新的中国互联网发展状况统计报告显示，过去一年中，超过 60%的中国互联网用户的计算机曾被入侵过。从 1997 年因为印尼排华而引发的黑客攻击事件，到去年 5 月间因为中美撞机事件而引发的中美黑客大战，遭受攻击劫难的计算机数以千计，互联网一度陷入“混乱”的局面。网络在为人们提供便利、带来效益的同时，也使人们面临着信息安全方面的巨大挑战。我国加入 WTO 后，在网络安全方面将面临更大的压力和挑战。

为了消除网络上弥漫的不安定因素，遏制黑客肆无忌弹的攻击行为，网络安全技术逐渐发展并形成了完整的体系。针对系统及数据安全，密码学技术的应用逐渐成熟起来；针对网络入侵，防火墙技术和入侵检测系统得以发展和完善；为了消除系统隐患，人们采用了各种主动审核技术，包括漏洞扫描、动态响应等。

必须承认的是，解决网络安全的问题并没有一劳永逸的万全之策。技术在不断地发展，相应的系统和网络的问题也在不断地出现；黑客的攻击手段不断地更新变换，而相应的防御技术也在不断发展。从现实角度考虑，黑客要进行攻击，必须了解网络及系统中的漏洞，而管理员要进行防御，就必须了解黑客的习性及攻击手段。本书的主旨正是通过剖析黑客的攻击手段和典型的系统及网络漏洞来引导读者全面地掌握防范黑客攻击的技术。

一、关于本书

笔者提笔的初衷是想整理一下硬盘上堆积的大量软件及技术资料，后来发现，关于网络安全这么一个庞大复杂的知识体系，一篇简单文档是远不能完全覆盖的，以至于最终形成了一册厚厚的书籍。按照笔者的思路，写作本书的过程，一方面是一个将防范黑客攻击的技术进行系统化、条理化的过程，另一方面也是一个庞杂的工具库及资料库的归整过程。

在写作本书的过程中，笔者特别注重实践操作与底层技术的紧密结合。从大的框架来看，本书以分析黑客攻击的步骤为写作线索，在对每一种黑客攻击手段进行深入刨析的同时，详细描述了相应的防御对策。从实用性来看，本书特别强调可操作性，介绍了大量有关攻击和防御技术的实用工具及实例，力求使读者在实践的环境中建立对网络安全技术的深刻认识。本书的另一个特点，就是将与网络安全相关的各种基本知识穿插在正文内容中间（以楷体字体显示）介绍，例如关于 DNS、ICMP、FTP 的基本知识等，有相应的基本知识作为铺垫，读者将对每一种网络安全技术有更深入的理解。

阅读过程中，读者可以选择不同的阅读方法。习惯于从头至尾连续阅读的，可以先浏览基本知识的介绍部分，回顾一下曾经掌握或已经略显生疏的技术内容，这对于加深正文部分的理解很有帮助；而不想被插入的基本知识干扰了对正文理解的（因为基本知识相对正文内容毕竟是较独立的部分），则完全可以略过这一部分，直接阅读正文内容，当出现对某些基本

常识理解上的困难时，可回过头来，在基本知识部分中寻找相应的解答。

一本书是不能覆盖所有网络安全涉及的内容的，因此本书提出一种可扩展的知识框架体系，通过所提供的大量经过归整的工具及资料，让读者有更多机会去进行实践操作，或者进行更深入的研究。一定程度上讲，本书只是引领读者进入黑客攻防技术领域的一个契机，通读本书，读者虽然不可能一下子成为真正的黑客或者网络安全专家，但至少可以知道怎样成为黑客或网络安全专家，剩下的，就需要自己不断地去积累了。

二、本书的读者对象

本书面向有一定网络技术基础的网络安全爱好者，或者从事网络系统管理的专业技术人员。只要您对技术原理从来都带有孜孜不倦的追求热情，只要您真的想了解并掌握网络安全攻防技术，那么，从这里开始，循序渐进，本书一定会让您有所收获的。

三、本书的组织结构

本书依据黑客完整攻击行为中的不同阶段安排章节结构，在介绍黑客攻击手段的同时，有针对性地提供相应的防御对策，最后系统地给出了一个完整的网络安全解决方案。

本书共 6 章，具体内容如下所述。

第 1 章（黑客概述）：介绍了黑客的确切定义、发展过程和传奇故事。

第 2 章（踩点——搜索信息）：踩点即通过多种途径获得有关目标系统的大量信息，包括域名、IP 地址范围、邮件地址、用户账号、网络拓扑、路由跟踪信息、系统运行状态等。进行踩点的工具有很多种，有以命令行方式运行的 finger、whois、nslookup、dig、ping、traceroute、pathping 工具等，也有以图形界面方式运行的 VisualRoute、SmartWhois、SamSpade、NeoTracePro、NetScanTools 工具等。所有这些工具所采集得到的信息，都可以用到进一步的探测及攻击活动中。本章最后提出了两方面的踩点防御对策，一方面是关于 DNS 服务器安全性的内容，另一方面是关于禁止 ping echo 的安全设置的内容。

第 3 章（扫描——探测漏洞）：如果说踩点阶段获得的是诸如“姓甚名谁”的信息，那么扫描阶段所要获得的就是“以往病史”及“目前身体状况”一类的信息，这些敏感或漏洞信息可以被黑客直接利用来进行攻击。本章即对扫描阶段黑客可能施展的各种手段进行分类介绍，包括端口扫描、操作系统类型探测、针对特定应用及服务的漏洞扫描（包括 Web 漏洞扫描、Windows 漏洞扫描、SNMP 漏洞扫描、RPC 漏洞扫描等），在分析各种扫描手段技术原理的同时，对典型的扫描工具进行了分类介绍，包括专用的扫描器以及综合性安全评估工具，例如 Nessus、ISS、CyberCop Scanner 等。在技巧方面，本章还介绍了扫描过程中的隐藏技术。最后，本章提供了针对扫描攻击所能采取的防御对策，包括扫描监测工具及个人防火墙的使用。

第 4 章（嗅探——Sniffer 技术）：嗅探是黑客攻击过程中较为灵活的一种手段，如果满足必要的条件，通过嗅探，黑客可以获得大量的敏感信息，包括用户账号、登录口令、邮件内容等。本章即对嗅探技术展开深入讨论，包括其原理、嗅探器的软件实现方式、典型的嗅探工具、交换网络嗅探技术等。最后，本章突出介绍了相应的安全对策，包括嗅探检查方法、防止 ARP 欺骗的方法、各种数据加密通道技术（SSH、SSL、VPN）、邮件加密方法（PGP）等。

第 5 章（攻击——直捣龙门）：前面几章介绍的是黑客攻击活动中的刺探阶段，本章介绍黑客实施攻击阶段的内容。本章首先对一般性的攻击方法进行归类介绍，这些方法是超乎特定系统并普遍存在的，包括 DoS 攻击、DDoS 攻击、口令破解攻击、网络欺骗类型的攻击、会话劫持攻击、缓冲区溢出攻击等。然后介绍黑客依据获取访问权进行的提升权限（获取控制权）、消除痕迹、留置后门等纵向行为模式，本章分别对 Windows 系统及 UNIX 系统攻击方法展开了讨论，并提供了相应的攻击对策，包括系统管理及配置要点以及典型的安全防护工具。其次，本章还专门介绍了网络蠕虫。最后，本章以 Snort 为例，介绍了入侵监测系统的发展及应用情况。

第 6 章（对策——网络安全整体解决方案）：前几章里介绍的防御对策，多是针对特定攻击手段或系统漏洞而提出的，这些零散的对策并不足以构成完整的安全解决方案。本章从系统和整体的高度出发，介绍了一种完整的网络安全解决方案，包括网络安全目标及模型的确立、安全风险分析、安全策略制订、安全机制选择、弱点评估、应急处理、安全管理等。

四、其他

笔者张耀疆（MCSE+Internet，MCSD，CCNA），1995 年本科毕业于北京航空航天大学自动控制系，之后几年里，先后在深圳、西安等地多家公司从事软件开发及网络安全技术研究工作，2000 年就读上海交大网络安全专业研究生，并担任上海保晨及 Sun 公司技术顾问。多年积累的技术开发及咨询服务经验，使笔者对网络安全有了全面而深刻的理解。

本书在写作过程中得到了顾水林、程立、李刚、付念东、邱克民等许多朋友及师长的支持和帮助，在此笔者向他们表示真挚的感谢。特别是笔者的导师汪为农教授，他的不倦教导及指点给予了笔者极大的鼓励。

由于水平所限，加上实验条件的限制，书中疏漏之处在所难免，恳请读者批评指正，欢迎联系交流。

E-mail 地址：colababy@263.net.cn

OICQ：3304964

作　者

目 录

第 1 章　黑客概述

1.1　什么是黑客

“黑客”是“Hacker”这个英语名词的泊来品，它源于对应的动词“hack”，意思是“劈砍”。引申一下，“Hacker”最直接的意思就是“劈或砍东西的人”。有意思的是，只要简单地在金山词霸中输入“Hacker”来进行查询，就可以得到对“Hacker”的多种解释：“计算机窃贼”、“砍伐工”、“剁碎机”、“从网络中擅自存取的人”等。在日本出版的《新黑客词典》中，对“黑客”是这样定义的：“喜欢探索软件程序奥秘，并从中增长了其个人才干的人。他们不像绝大多数电脑使用者那样，只规规矩矩地了解别人指定了解的狭小的一部分知识”。在 Open Source（开放源码运动）旗手 Eric S. Raymond 的《The New Hacker's Dictionary》一文中，对“Hakcer”的解释包括了下面几类人（参见网址 http://tuxedo.org/jargon/jargon.html）：

- 那些喜欢发掘程序系统内部实现细节的人，在这种发掘过程中，他们延伸并扩展着自己的能力，这和许多只满足于学习有限知识的人是截然不同的。
- 那些狂热地沉浸在编程乐趣中的人，而且，他们不仅仅在理论上谈及编程。
- 一个高超的程序设计专家。
- 一个喜欢智力挑战，并创造性地突破种种环境限制的人。
- 一个恶意的爱管闲事的家伙，他试图在网络上逡巡溜达的同时发现一些敏感的信息。

对最后一类人，Eric S. Raymond 赋予其更恰当的一个称谓，那就是“Cracker”，也就是我们常说的“骇客”，指那些乐于破坏的家伙。当他们在给这个社会制造着麻烦和噱头的同时，就只能被冠以“骇客”之名了。正是因为“骇客”的存在，纯正而古老的黑客精神才愈来愈被人们曲解，但在真正崇尚黑客精神的一类人眼里，“骇客”（Cracker）与“黑客”（Hacker）是如此的泾渭分明、不可混淆。

1.2　黑客文化的发展

黑客最早起源于 20 世纪 50 年代麻省理工学院的实验室中。那时，一些才华横溢的学生结成不同的课题小组，通霄达旦地在实验室操作机器，他们擅长抓住瞬间的思想灵感去尽情地发挥，对解决难题充满了由衷的热爱。他们刻苦、勤奋、精力充沛，甚至有些玩世不恭。20 世纪 60 年代，黑客代指独立思考、奉公守法的计算机迷，他们利用分时技术使得多个用

户可以同时执行多道程序，这扩大了计算机及计算机网络的使用范围。20 世纪 70 年代，黑客倡导了一场个人计算机革命，他们发明并生产了个人计算机，打破了以往计算机技术只掌握在少数人手里的局面，并提出了计算机为人民所用的观点。这一代黑客是电脑史上的英雄，其领头人就是苹果公司的创建人史蒂夫·乔布斯。20 世纪 80 年代，黑客的代表是软件设计师，包括比尔·盖茨在内的这一代黑客为个人电脑设计出了各种应用软件。同一时期，随着计算机重要性的提高，大型数据库也越来越多，信息越来越集中在少数人手里，黑客开始为信息共享而奋斗，他们频繁入侵各大计算机系统，在提升着互联网共享精神的同时，也给网络的发展注入了众多不稳定的因素。

做为独特的群体，黑客们信奉着几十年一直延续下来的一种独特的文化理念。在这种滋生于网络的文化理念中，真正意义上的黑客，用技术手段来维护电脑和网络世界的宁静，构筑着网络的便捷和安全，他们是正义的侠士。他们所崇尚的所谓“黑客文化”强调的是信息共享的精神，这种精神恰是自由主义与个人英雄主义的结合。黑客们不断地创造（而不是破坏），不断地证明着自己，在解决问题与克服限制的过程中永远不知疲倦。

深入来看，黑客文化首先包含了一种自由不羁的精神。黑客们在网络上自由驰骋，他们喜欢不受束缚，喜欢挑战任何技术制约和人为限制。黑客们认为所有的信息都应当是免费的和公开的。黑客行为的核心目的，就是要突破强加给信息本身的种种限制。黑客就是那些在网络上对信息“劫富济贫”的人，他们从事黑客活动，意味着接受艰巨的智力挑战，意味着尽可能地使计算机的使用和信息的获得成为免费和公开的，意味着坚信完美的程序将解放人类的头脑和精神。其次，黑客文化也包含了反传统、反权威、反集权的精神，这是对 20 世纪 60 年代反主流文化价值观的继承。黑客们蔑视现行电子世界的行为规则，认为这些规则并不能起到维持法律秩序和保护公共安全的作用，相反只是为了获取利润和镇压异己，是不道德的，而他们自己是既有反抗精神又身怀绝技的天才，是电子时代的“侠盗罗宾汉”。

这个独特的群体也遵循着其特有的一套行为准则，美国学者史蒂夫· 利维在其著名的《黑客电脑史》中所指出的“黑客道德准则”（the Hacker Ethic）就是对其最深刻的表述。

（1） 通往电脑的路不止一条；

（2） 所有的信息都应当是免费共享的；

（3） 一定要打破电脑集权；

（4） 在电脑上创造的是艺术和美；

（5） 计算机将使生活更加美好。

可以看出，“黑客道德准则”正是这个独特的文化群体一直心照不宣地遵循着的“江湖规矩”。以这种“江湖规矩”作为参照，黑客们的行为特征也就清晰地呈现给我们了。

❑ 热衷挑战

黑客们多数都有很高的智商，至少在某些方面表现突出。他们喜欢挑战自己的智力，编写高难度程序、破译电脑密码给他们带来了神奇的魔力，认为运用自己的智慧和电脑技术去突破某些著名的、防卫措施森严的站点是一件极富刺激性和挑战性的冒险活动。

❑ 崇尚自由

黑客文化首先给人的突出感觉就是一种自由不羁的精神。黑客如同夜行的蝙蝠侠，任意穿梭于网络空间中。黑客在电脑虚拟世界发挥着自己极致的自由。他们随意登录世界各地网站，完成着现实生活中无法企及的冒险旅程，实现着个人生命的虚拟体验。正是这种对自由

的体验，使黑客如同吸毒上瘾一样，对网络入侵乐此不疲。

❑ 主张信息共享

黑客们认为所有的信息都应当是免费的和公开的，认为计算机应该是大众的工具，而不应该为有钱人所私有。信息应该是不受限制的，它属于每个人，拥有知识或信息是每个人的天赋权利。

❑ 反叛精神

黑客文化带有某种反叛世界的倾向，黑客们蔑视传统，反抗权威，痛恨集权，其行为模式深深地烙上了无政府主义的印记。互联网的一个显著特点是平等和共享，对于网络中存在着的许多禁区，黑客们认为是有违网络特征的，他们希望建立一个没有权威、没有既定秩序的社会，所以他们一般都喜欢与传统、权威和集权做永无休止的斗争。

❑ 破坏心理

黑客们要在网络空间来去自由、蔑视权威，就必然夹带着某些破坏举动。只有突破计算机和网络的防护措施才能随意登录站点；只有颠覆权威设置的程序才能反抗权威；也只有摧毁网络秩序才能达至人人平等的信息共享目标。当然，由于心理动机不同，不同黑客行为的破坏程度也是有区别的。

这样一种独特的黑客文化，必然孕育出黑客群体所独有的文化态度。

（1） 这个世界不断涌现出许多迷人的问题等待人们去解决；

（2） 一个问题不应该重复地被解决两次；

（3） 无聊而乏味的工作是可恶的；

（4） 自由是美好的，黑客们需要的是自由协作和信息共享，而不是专制和所谓的权威；

（5） 态度并不能成为能力的替代品，想成为黑客，只有态度是不够的，更重要的，还在于努力工作、倾心奉献、钻研和实践。

老一代的黑客精英，他们更多专注的是创造和奉献，在他们身上，体现更多的是真正的黑客精神，然而自由和共享在这个商业气息浓厚的现实社会里总显得如此弱不禁风，当人们为了追逐金钱和利益而不惜心力的时候，自由和共享就带有浓浓的理想主义色彩了。传统的商业社会是拒绝共享的，为了获得并独享更多利益，对各种信息加密和限制措施的使用就成了传统商业必然的手段，所谓的完全共享在商业社会中实际上意味着倒闭与贫穷。崇尚自由和共享的人们总是“矢志不虞”，他们要突破这些人为的限制，要破坏种种给信息设置的藩篱，于是，一个专门致力于搞破坏的群体就开始不遗余力大行其道了，不过，从他们身上，很少再能看到老一辈黑客崇尚创造的精神，相反，他们所表现的，除了破坏，还是破坏。这样一个群体，不光为社会所痛恨，就连承袭着传统黑客文化的“黑客”们也对此大为不齿，并极力将之归类为另一个阵营，那就是“Cracker”，也就是我们常说的“骇客”，他们不是创造者和建设者，而是真正意义上的破坏者。

1.3　关于黑客的传奇故事

提起黑客，就不能不说说关于黑客的一些光怪陆离的“事迹”。就像武侠小说吸引人们

进入一个成人的童话世界那样，有关黑客的种种传奇故事，在媒体或夸张或引申之后，听起来是那样的神乎其神，并散发着经久不息的独特魅力。这其中，最为经典的就是关于凯文·米特尼克（Kevin Mitnick）的传奇故事。

凯文·米特尼克，这个被奉为世界头号电脑黑客的传奇人物，很久以来，一直都是许多怀有叛逆和自由不羁精神的黑客群体的心中偶像。出生于1964年的凯文，从其15岁入侵北美空军防务指挥系统开始，短短十几年间，一次次给网络世界制造着麻烦，屡屡被捕但从没有放弃自己麻烦制造者的秉性。其传奇故事甚至成了好莱坞的蓝本题材而被搬上了银幕（1983年好莱坞拍摄的《战争游戏》）。

1964年，凯文·米特尼克出生在美国西海岸的洛杉矶。当他只有3岁的时候，由于父母离异，跟着母亲生活的米特尼克很快就学会了自立。虽然父母离异对米特尼克幼小的心灵造成了很深的伤害，使他性格内向、沉默寡言，虽然文化水平不高的母亲并没有很好的教育孩子的经验，但这些丝毫没有妨碍米特尼克超人智力的发育。事实上，在很小的时候，米特尼克就经常显示出他在日后成为美国头号电脑杀手所具有的天才和能力。

米特尼克小时候喜欢玩一种当时很流行的名为“拿破仑的滑铁卢”的游戏。根据专家的理论推算，最快需要78步才能完成游戏中的使命，而令人吃惊的是，年仅4岁的米特尼克只用了几天功夫，就证明了这一专家耗时长达1个月才能得出的结论。

13岁时，还在上小学的米特尼克喜欢上了业余无线电活动，在进一步接触电脑之后，数字世界所蕴涵的数理逻辑知识与他的思维方式仿佛天作之和。于是，米特尼克开始着迷于电脑和网络营造的数字空间，在那里，他可以暂时摆脱所厌恶的现实生活，并运用自己的天才去发泄着对现实世界的不满。

米特尼克最初开始显露其攻击秉性是在美国兴起社区电脑网络建设的阶段。在米特尼克所在的社区网络中，家庭电脑不仅和企业、大学相通，而且和政府部门相连，当然，那些通往禁地的关口通常都设置有密码。于是，米特尼克那种似乎与生俱来的“突破”的欲望开始“发作”了。他用打工赚的钱买了一台性能不错的电脑，然后就以超乎多数同龄人所能具有的耐心和毅力，试图破译美国高级军事密码。不久，年仅15岁的米特尼克闯入了“北美空中防务指挥系统”，他翻遍了美国指向前苏联及其盟国的所有核弹头的数据资料，然后又悄无声息地溜了出来。这一“事迹”，随即成为黑客历史上最为经典的案例之一，甚至被好莱坞搬上了银幕。

成功突破“北美空中防务指挥系统”的防线之后，米特尼克信心大增，随后不久，他又进入到著名的“太平洋电话公司”设在南加利福尼亚州的通信网络，并随意更改这家公司的用户信息，给太平洋公司以及其众多知名用户带来了不小的麻烦。

对太平洋公司失去兴趣之后，米特尼克的目光瞄准了联邦调查局，他开始频繁地进出联邦调查局的电脑网络。一次，他发现特工们正在调查一名电脑黑客，便饶有兴趣地偷阅起调查资料来。结果令他大吃一惊：被调查者竟然是他自己！米特尼克立即施展浑身解数，破译了联邦调查局“中央电脑系统”的密码，并且每天仔细地查阅“案情进展情况报告”。很快，米特尼克就对此不屑一顾起来，他嘲笑这些特工人员漫无边际的搜索，并恶作剧式地将几个负责调查的特工的档案调出，然后全都涂改成了十足的罪犯。

不过，联邦调查局的特工人员最终还是将米特尼克捕获了。当人们得知这名弄得联邦特工狼狈不堪的黑客竟是一名不满16岁的孩子时，无不惊愕万分。这时候，人们更多考虑的并非米特尼克所制造的种种极俱威力的破坏，而是惊叹于米特尼克不同寻常的天才，许多善良

的、并不了解真相的人们纷纷要求法院对他从轻发落。也许是由于网络犯罪还很新鲜，法律上鲜有先例，法院顺从了“民意”，仅仅将米特尼克关进了“少年犯管教所”，很快，米特尼克就被假释了。

自由后的米特尼克并未改邪归正，电脑网络对他的诱惑实在是太大了。这次，他把目光投向了一些信誉不错的大公司。在很短的时间里，他连续进入了美国 5 家大公司的网络，不断发出让人愤怒的错误账单，把一些重要合同涂改得面目全非。

1988 年，因为 DEC 指控他从公司网络上窃取了价值 100 万美元的软件并造成了 400 万美元损失，米特尼克再次被执法当局逮捕。他甚至未被允许保释，心有余悸的警察当局认为，只要接触键盘，他就会对社会构成威胁。

在一年刑满后，米特尼克出狱了，不过，联邦政府始终认为他是对社会的一个威胁，他的一举一动，都在严密的监视之下。这让许多有心利用他高超电脑技术的雇主都望而却步，这不能不说是一个遗憾。

1993 年，一直对米特尼克心有不安的联邦调查局甚至设下圈套，故意引诱米特尼克重施故伎，以便把他再次抓进监狱。面对这种“诱惑”，米特尼克很快就落入了圈套。但头号黑客毕竟不凡，他打入了联邦调查局的内部网，发现了这个圈套，在逮捕令发出之前就逃跑了。联邦调查局立即在全国范围对米特尼克进行通缉。其后两年中，米特尼克与联邦调查局就一直玩着猫捉耗子的游戏。这期间，米特尼克成功地入侵了摩托罗拉、Novell、诺基亚、Sun 等多家高科技公司的计算机系统，盗走了大量的软件和数据。甚至有报道说，在逃跑过程中，米特尼克设法控制了加州的一个电话系统，以便随时窃听追踪他的警探的行踪。

1994 年圣诞节，米特尼克向圣迭戈超级计算机中心发动了一次攻击，《纽约时报》称这一行动“将整个互联网置于一种危险的境地”。这次攻击的对象，包括一个因为米特尼克而一举成名的人物，即被称作“美国最出色的电脑安全专家之一”、在该中心工作的日籍计算机专家下村勉。米特尼克这种“在太岁头上动土”的举动极大地触怒了下村勉，他下决心帮助联邦调查局把米特尼克缉拿归案，于是，在米特尼克和下村勉之间，演绎出了一场颇为曲折的“江湖龙虎斗”。先是米特尼克在下村勉的电话留言机上留下这样的挑衅话语：“诅咒你！我的技术是最棒的！……”，个性倔强的下村勉显然不能容忍这样的挑衅行为，他采用一种特殊的跟踪方法，让自己的跟踪举措隐形，并通过捕获米特尼克的无线电话指令来发现电波波长的真正来源。

时间到了 1995 年情人节之际，经过不懈的努力，下村勉终于发现了米特尼克的踪迹，并通知联邦调查局，在北卡罗来纳州罗利市一片布满低级公寓的街区内将其逮捕。

米特尼克与下村勉的第一次会面极具历史意义。1995 年 2 月，在北卡罗来纳州的法庭上，带着手铐的米特尼克向出庭作证的下村勉由衷地说：“你好啊下村，我钦佩你的技术。”

作为一个处处制造混乱和破坏的电脑天才，米特尼克被指控违反了高达 23 条的法律，对于每一条他所违反的法律，都足以判处 20 年的监禁。后来，在米特尼克众多支持者的不懈努力之下，法庭仅仅判处他 5 年的监禁。当然，心有余悸的三位美国联邦法官一致否决了米特尼克的假释要求，按法官的话说：“如果让米特尼克假释出狱，无异于放虎归山，整个美国，甚至整个世界都要乱了。”

2000 年 1 月 21 日，凯文·米特尼克获释，根据美国法院的规定，在很长一段时期内，他必须处于严密的监控之下。他被禁止从事计算机行业的工作，禁止接触任何与电子有关的物品，包括计算机、手机、互联网等，甚至连入学进修也不能选择计算机专业。