《计算机安全超级工具集》

图书基本信息

书名：《计算机安全超级工具集》

13位ISBN编号：9787302194392

10位ISBN编号：7302194394

出版时间：2009-6

出版社：清华大学出版社

作者：Bryan Burns,Jennifer Stisa Granick,Steve Manzuik,Paul Guersch,Dave Killion

页数：700

译者：Nicol 李展,贺民,周希

《计算机安全超级工具集》

前言

有人说人与动物的根本区别，就是会制造和使用工具。亚里士多德有这样一句名言，“给我一个支点，我就可以翘动地球”。理论上这是可行的。当然，仅仅有支点是不够的，还需要使用杠杆，杠杆就是工具，我们可以看到工具的重要作用。其实，工具无处不在。我们吃饭，需要工具（筷子，碗等）；我们工作，需要工具（电脑，鼠标等）；我们出行，需要工具（自行车，公交车等），就是简单地钉几页纸，也需要钉书器或曲别针之类的小工具，画一条直线、画一个圆呢，会需要板尺和圆规……工具，可以说在我们的生活中随时随地为我们服务，提供帮助。当然，没有这些工具，我们也可以生活或工作，比如，画直线，画圆，徒手完全可以，但总不会有使用板尺画的线条那么笔直，也不会有使用圆规画的圆圈那么圆；出行走路也可以，但总不如坐车的速度快。　　计算机软件工具，可以说浩如烟海。本书所选的工具，仅仅针对安全问题。这是因为，在使用电脑的过程中，安全问题已经成为人们不可忽视的重要问题。现在，随着Internet的流行，很少有不联网的孤岛一样的计算机，人们在从网络中共享信息、轻松聊天、互通邮件等受益的同时，也面临着许多风险。影响到计算机系统安全的不仅仅是简单的病毒，还有大量来自网络的攻击，也许在你不知不觉中，黑客和垃圾邮件传播者可能正在悄悄利用你的计算机，把它作为任人宰割的“肉鸡”，他们悄悄入侵，用恶意软件获取信息，包括邮件程序。一旦你上线，他们就可以上网记录，盗取信息，并控制你的邮箱发送垃圾邮件，使你成为僵尸网络中的一部分。而对于企业来说，网络安全则更为重要，因为它甚至有可能影响到企业的效益和生存。计算机安全的重要性再怎么强调也不过分。　　本书讲解的辅助网络安全的工具，有免费软件，还有商用软件，它们都极为优秀。本书讲解的诸多网络安全工具都是作者精挑细选的，也许你正在烦恼苦思冥想的安全难题，使用本书介绍的一个看起来不起眼的小工具就可以迎刃而解了。这本书最主要的作用就是，书中介绍的工具可以帮助您提高效率，保护好计算机和网络，更出色地完成任务。

《计算机安全超级工具集》

内容概要

《计算机安全超级工具集》有23个章节，内容彼此关联，详细说明了现在世界上最优秀的安全工具，不管是对于黑帽技术，还是对白帽防御策略，都极具价值。正文内容中，针对免费软件和商用工具，范围涉及中级的命令行操作，甚至深入到相关软件的高级编程知识，都有提示、技巧以及“如何做”的忠告信息。如果您可以与世界上天才的计算机安全工程师坐在一起，询问您的网络安全问题，会感觉如何?《计算机安全超级工具集》就能让您实现这个梦想！在《计算机安全超级工具集》中，Juniper网络安全工程团队的成员，还有一些外聘的专家，揭示了如何使用、处理和推广最流行的网络安全应用、实用程序和工具，它们适用于Windows、Linux、MacOS X和Unix平台。
《计算机安全超级工具集》涉及的主要内容有：
· 检测工具——网络扫描工具，比如nmap；漏洞扫描；局域网检测；无线检测；自定义数据包生成。
· 渗透工具——远程计算机的自动渗透，比如Metasploit框架；查找无线网络的工具；操作shell代码的技巧和工具。
· 控制工具——作为后门使用的工具；已知rootkits的审查。
· 防御工具——基于主机的防火墙；主机加固；与SSH的通信安全；电子邮件安全和反恶意软件；设备安全测试。
· 监视工具——抓包和分析数据包的工具；使用Honeyd和snort进行网络监视；生产服务器的主机监视，用于文件更改。
· 发现工具——包括The Forensic Toolkit、Sys Internals和其他流行的法律工具；应用程序干扰器和干扰技术；使用诸女7Interactive Disassembler和ollydbg这样的工具进行二进制逆向工程的技巧。另外，《计算机安全超级工具集》还有斯坦福大学法律教授编写的有关网络安全的相关法律知识，这些内容实用而且及时有效，这使得《计算机安全超级工具集》成为一座网络安全信息的金矿。

《计算机安全超级工具集》

书籍目录

《计算机安全超级工具集》

章节摘录

第一部分 法律和道德　　1 法律和道德问题　　在2005年的夏天，来自世界各地的系统管理员以及安全研究者汇聚内华达州拉斯维加斯召开了黑帽（Black Hat）会议，这是世界上最大的计算机安全会议之一。在会议第一天的上午，Michael Lynn，　　的作者之一，被安排做关于思科（Cisco）路由器安全隐患的发言。这些安全隐患是严重的：攻击者能够接管机器，并且能够驱使它们运行该攻击者想要运行的任何程序。　　思科公司不想让Lynn进行这样的介绍。在与Lynn的老板进行最后的协商之后，ISS公司决定要Lynn更改他的发言。在发言的前夜，一小队法警集中到会址，并且没收了包含有Lynn所作发言的幻灯片的光盘，同时没收了印有会议议程的印刷品。然而，Lynn仍然想进行最初的发言。他认为，系统管理员了解到这种路由器的安全隐患至关重要。一次简单的软件升级就能够修复该问题，但很少人知道这个安全隐患。Lynn认为，揭露这个隐患，可以使Internet更加安全。因此，他辞去了他在ISS的工作，并且进行了他最初计划进行的发言。　　当晚，思科公司和ISS公司起诉了Lynn以及黑帽会议。　　我们处在信息时代，这意味着，信息就是金钱。现在，我们有比25年前更多的法律保护信息，同时也有更多的信息受到法律的保护。思科和ISS公司声称，Lynn违反了这些法律、侵犯了知识产权、泄漏了商业机密，并且违反了他与ISS签订的雇佣合同。　　Lynn向我咨询，因为我在最近十年研究了这些涉及计算机安全的法律。我为程序员、计算机黑客以及研究者提供咨询，帮助他们摆脱麻烦，并且，当有麻烦找上客户时，为他们进行代理。我就计算机侵权法律、弱点揭露以及知识产权保护问题，在黑帽会议上、国家安全局、海军研究生学校、Internet安全论坛以及澳大利亚计算机紧急事件应对小组（Computer Emergency Response Team）会议上进行过发言。我担任了九年犯罪防止律师，并且在过去六年中在斯坦福法学院（Stanford Law Sch001）全职任教。

媒体关注与评论

从1993年首次出版本书以来，我一直在看它。我一直渴望，一直在等待它。感谢本书，它字字珠玑。感谢这些才华横溢的作者。” ——Pelter“ Mudge ”Zatko

《计算机安全超级工具集》

精彩短评

1、对我来说太难了。但是那些渗透工具和后门工具真的是可以随便用的吗？！
2、计算机安全超级工具集
3、昨天惊喜发现还有中文的，收了
4、juniper的安全工程师写的图书，介绍各个方面的安全工具，翻译生硬，工具已经有些陈旧了，可以参考。
5、scapy大法好。。以后网络实验都靠他了//翻译是一坨翔啊。看看139页写的是啥玩意儿啊//读完 计算机网络自顶向下 然后再上这本书，简直神了。。
6、晦涩

《计算机安全超级工具集》

版权说明