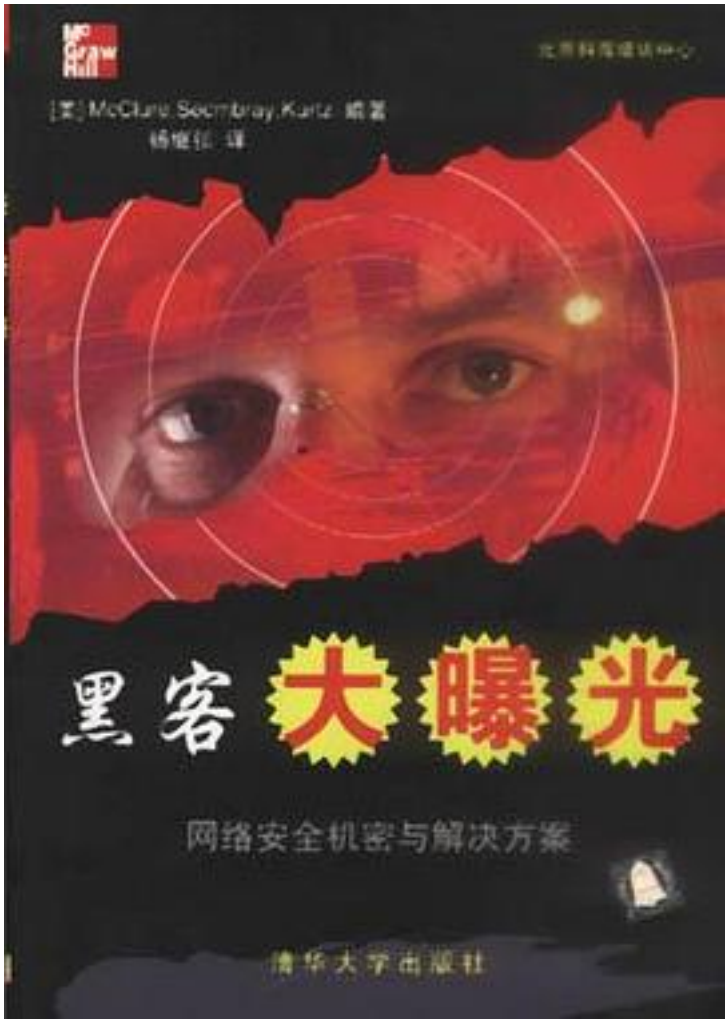
黑客大曝光



黑客大曝光_下载链接1_

著者:Michael A.Davis

出版者:机械工业出版社华章公司

出版时间:2011-6-10

装帧:

isbn:9787111340348

抵御恶意软件和Rootkit不断掀起的攻击浪潮！《黑客大曝光：恶意软件和Rootkit安全

》用现实世界的案例研究和实例揭示了当前的黑客们是如何使用很容易得到的工具渗透和劫持系统的，逐步深入的对策提供了经过证明的预防技术。本书介绍了检测和消除恶意嵌入代码、拦截弹出式窗口和网站、预防击键记录以及终止Rootkit的方法，详细地介绍了最新的入侵检测、防火墙、蜜罐、防病毒、防Rootkit以及防间谍软件技术。

《黑客大曝光：恶意软件和Rootkit安全》包括以下内容：

- 理解恶意软件感染、生存以及在整个企业中传染的方法。
- 了解黑客使用存档文件、加密程序以及打包程序混淆代码的方法。
- 实施有效的入侵检测和预防程序。
- 防御击键记录、重定向、点击欺诈以及身份盗窃威胁。
- 检测，杀死和删除虚拟模式、用户模式和内核模式Rootkit。
- 预防恶意网站、仿冒、客户端和嵌入式代码攻击。
- 使用最新的防病毒、弹出窗口拦截程序和防火墙软件保护主机。
- 使用HIPS和NIPS识别和终止恶意进程。

作者介绍:

Michael A. Davis是Savid Technologies公司的CEO，该公司是一家全国性的技术和安全咨询公司。由于Michael将snort、ngrep、dsniff和honeyd这样的安全工具移植到Windows平台，因此他在开源软件安全界声名卓著。作为Honeynet项目成员，他为基于Windows的honeynet（蜜罐）开发了数据和网络控制机制。Michael还是sebek for Windows的开发者，这是一种基于内核的honeynet数据收集和监控工具。Michael曾经在领先的防病毒保护和漏洞管理企业—McAfee公司担任全球威胁高级经理，领导一个研究机密审查和尖端安全的团队。在McAfee工作之前，Michael曾在Foundstone工作过。

Sean M. Bodmer是Savid Corporation公司的政府项目主管。Sean是一位活跃的honeynet研究人员，精于分析恶意软件和攻击者的特征、模式和行为。最为引人注目的是，他花费了多年的时间来领导高级入侵检测系统（honeynet）的运作和分析，这一系统能够捕捉和分析入侵者及其工具的动机和目的，从而生成对进一步保护用户网络有价值的信息。在过去的10年中，Sean已经为华盛顿特区的多个联邦政府机构和私人公司负责过各种系统安全工程。Sean在全美国的业界会议，如DEFCON、PhreakNIC、DC3、NW3C、 Carnegie Mellon CERT和Pentagon安全论坛上发表过演讲，主题包括对攻击特征和攻击者的剖析，这些剖析能够帮助识别网络攻击的真正动机和意图。

Aaron LeMasters（乔治·华盛顿大学理科硕士）是一位精通计算机取证、恶意软件分析和漏洞研究的安全研究人员。他在职业生涯的头5年用在保护不设防的国防部网络上，现在他是Raytheon SI的高级软件工程师。Aaron乐于在大的安全会议（如Black Hat）和较小的区域黑客会议（如Outerzone）上分享研究成果。他更愿意关注与Windows内部构件、系统完整性、逆向工程和恶意软件分析相关的高级研究和开发问题。他是一位热心的原型构造者，很喜欢开发增强其研究趣味性的工具。在业余时间，Aaron喜欢打篮球、画素描、摆弄他的Epiphone Les Paul电吉他，以及和妻子一起去纽约旅行。

・・・・・・(收起)

黑客大曝光_下载链接1_

标签

网络安全

黑客

安全

hacker

计算机科学

计算机

计算机技术

已入手

评论

有些启发意义 但是实际价值不大

不太适合初学者，攻击原理 技术 和对抗方案交错在一起，稍有点乱。
初学者更适合另一本书：恶意软件、rootkit和僵尸网络

黑客大曝光_下载链接1_

书评

黑客大曝光_下载链接1_