<<Linux黑客大曝光>>

图书基本信息

书名：<<Linux黑客大曝光>>

13位ISBN编号：9787302242451

10位ISBN编号：7302242453

出版时间：2011-1

出版时间：清华大学

作者：安全研究社团

页数：579

前言

我对安全的兴趣开始于小时候。
那时，我的父亲加入了某著名大学的一个博士项目，这让我非常幸运。
当他在做研究时，我在那儿接触了许多的系统（有一台Vax 11/780，还有其他的系统）。
在实验室的那几年，我有了一台个人的Commodore 64电脑（注——Commodore International公司在1982年8月发行的一款8位家用电脑），还有一个300 bps的modem（调制解调器），能够访问神奇的UUCP互联世界。
我成功完成的第一个黑客之举，就是写一个登录脚本，模拟了一次不是很成功的登录，并将那个受害者输入的用户名和密码写入到了一个文件中。
这次攻击使得我可以在没有父亲监管的情况下任意登录那台系统。
这次经历，以及后来的经历，教我懂得了无效的安全控制的许多知识。
这激发了我去掌握更多的知识。
在1992年，我开始成为一名系统管理员，为一家小工程公司工作。
我负责大约30台工作站、一个使用UUCP拨入的Email供稿的（feed）BBS网站、一些SCO Unix服务器，以及一台Novell Netware服务器。
一段时间以后，公司要求我将这个小型网络接入Internet。
这时，我正好在学习Linux和IP伪装的共享能力方面的技术。
接下来的几年，Linux成为了我工作的核心，在很多项目中我都使用的是Linux系统，包括更新Novell和SCO服务器。
这段时间，大部分的IT厂家都很乐意简单地保持系统的正常运作。
任何安全控制都被认为有益的，然而却没有一个标准化的方式去衡量这样的有效性。
这是安全在私营企业中的一段绝对黑暗时期，因为安全已经普遍地被认为是一种高不可攀的艺术形态。
安全，已被束之高阁。

<<Linux黑客大曝光>>

内容概要

《linux黑客大曝光：linux安全机密与解决方案》第三版是一个全新的版本。
由isecom安全研究社团中linux各领域的专家根据最新、最全面的研究成果对其进行了彻底地重写，包括linux 2.6内核新增加的诸多安全功能。
isecom是知名的osstmm方法学手册的编著者，专注于提供有关安全性方面的全方位严谨思考和科学论证方法。
　本书涵盖的内容十分丰富，包括安全控制、安全分析方法，以及linux系统、数据网络、网络拨号、voip、蓝牙、射频识别、辐射攻击、可信计算、web应用攻击、邮件服务、域名服务、c代码静态分析、linux内核等领域的黑客攻防技术。
书中的所有组织材料，包括入侵案例都是最新的，在写作中遵循着“黑客大曝光”系列的一贯思路：每章以一个入侵案例展开，然后阐述这一领域的基础知识、可能发生的攻击，最后给出防范措施和安全对策。
各领域内容相互独立，因此便于读者针对某一领域进行专门学习。
　本书面向各行各业、政府机关、大专院校关注信息安全的从业人员，是linux信息系统安全专业人士的权威指南，也可作为信息安全相关专业的教材教辅用书。

作者简介

ISECOM成立于2001年1月，是一个开放的、非营利的安全研究组织，以安全研究为使命。
参与编写本书的项目组也参与了其他的ISECOM研究项目，比如开源安全测试方法手册(OSSTMM)、Hacker Highschool、专业安全认证及培训(OPST、OPSA、OPSE、OWSE)等。

<<Linux黑客大曝光>>

书籍目录

章节摘录

插图：OSSTMM的研究人员定义，最简单形式的安全不涉及风险，而是与保护有关。
这也是为何他们在探讨安全的过程中提及保护的原因。
他们得出的结论是，安全的最佳建模为“资产与威胁的分离”。
这一论述在讨论是否是网络诈骗、或是轻微盗窃罪，是否建立退休基金这些安全问题时得到广泛的应用，在每一类安全问题中，安全都将资产与威胁分离。
这不难理解，因为对于任何一种威胁的最好防御便是避免它，不论是通过远离它还是消除它的方式。
安全是资产与风险的分离。
通过军事力量实现的安全通常意味着摧毁威胁。
一个不具有威胁性的威胁就不再是威胁。
所以想要为资产规避威胁，您可以选用以下三种方式：物理上转移资产或将资产与威胁分离；摧毁威胁；移动或损毁资产。
就现实情况而言，损毁资产是不可取的，而摧毁威胁又往往非常复杂甚至是非法的。
只有分离二者通常是可以实现的。

媒体关注与评论

本书引导读者以一个实用的、现实世界的方法，帮助他们理解所面临的具体风险继而采取恰当的缓解措施。

——Jake Kouns CISSP CISM CISA

<<Linux黑客大曝光>>

编辑推荐

《Linux黑客大曝光:Linux安全机密与解决方案(第3版)》：无论您将Linux操作系统用于桌面操作系统、互联网服务、通信或是无线服务，《Linux黑客大曝光:Linux安全机密与解决方案(第3版)》都可以帮助您加固您的Linux网络的安全。

《Linux黑客大曝光(第三版)》基于ISECOMA9研究方法完全重写，由各领域专家组成的社团提供了最新、最全面的安全内容。

根据ISECOM最新的安全研究成果，《Linux黑客大曝光:Linux安全机密与解决方案(第3版)》完整而详细地讲述了怎样把入侵者阻挡在Linux系统外面，以及怎样避免Linux系统受到各种类型的攻击。

利用OSSTMM最新揭示的攻击及其防范措施来加强Linux安全基于Linux平台的PSTN、ISDN和PSDN攻击技术强化Linux系统上的VoIP、蓝牙、RF、RFID和IR设备安全阻挡Linux信号干扰、克隆和窃听攻击应用可信计算和密码学工具构建最佳防御系统修复DNS、SMTP和Web 2.0服务存在的漏洞防止SPAM、木马、网络钓鱼、DOS和DDoS攻击利用静态分析及霍尔逻辑方法查找和修改C代码里的错误

版权说明