<<灰帽攻击安全手册>>

图书基本信息

书名：<<灰帽攻击安全手册>>

13位ISBN编号：9787302146155

10位ISBN编号：7302146152

出版时间：2007-4

出版时间：清华大学出版社

作者：哈里斯

页数：409

字数：579000

<<灰帽攻击安全手册>>

内容概要

灰帽黑客在网络安全中代表发现漏洞但不利用漏洞进行攻击，而是与软件厂商协作寻找解决方案的人。

本书由多位安全领域的著名专家编写，按部就班地描述了灰帽黑客适用的道德、法律、操作过程、使用的工具和方法，旨在使你成为一个合格、全面的正义黑客。

全书分为4大部分共15章。

第1部分从道德规范和法律的角度介绍正义黑客，包括相关制度、工作步骤以及正确的漏洞发现过程，这些内容在同类书中极少涉及；第2部分介绍了渗透测试的过程与工具，包括建立测试团队和实验室、在工作中合法地保护自己、嗅探工具和渗透测试工具的合理使用；第3部分讲解各种攻击方法，有使用编程技巧对Linux系统的缓冲区、格式串和堆进行攻击，创建shellcode攻击，编写对Windows漏洞的攻击，并对代码逐行分析、点睛技巧，也是同类书难以寻觅；第4部分主要介绍各种漏洞分析方法和工具，包括被动分析，在源代码和二进制文件中识别漏洞并打补丁，对软件进行逆向工程、杂凑等。

本书涵盖了Linux和Windows系统，原理和技术并重，涉及面广，是信息安全管理人员、程序员以及对黑客技术感兴趣读者的必备工具书。

<<灰帽攻击安全手册>>

书籍目录

第1部分 泄密的道德 第1章 正义黑客的道德规范 1.1 本书内容与正义黑客类图书的关系 1.2 关于黑客书籍和课程的争论 1.3 攻击者为什么有机可乘 1.4 摘要 第2章 正义黑客与法制 2.1 与计算机犯罪相关的法律 2.2 摘要 第3章 完全而道德的揭秘 3.1 不同的团队和观点 3.2 CERT工作流过程 3.3 完全公开策略（RainForest Puppy策略） 3.4 互联网安全组织 3.5 矛盾仍然存在 3.6 案例研究 3.7 从现在开始，我们应该做什么 3.8 摘要第2部分 渗透测试与工具 第4章 渗透测试过程 4.1 测试的种类 4.2 如何开始评估 4.3 评估过程 4.4 摘要 第5章 超越《黑客大曝光》：当今黑客的高级工具 5.1 扫描之“过去的美好时光” 5.2 踩点：过去和现在 5.3 嗅探工具 5.4 嗅探和攻击LAN Manager登录凭据 5.5 摘要 第6章 自动化渗透测试 6.1 Python技巧 6.2 自动化渗透测试工具 6.3 摘要第3部分 攻击 第7章 编程技巧 7.1 编程 7.2 C语言 7.3 计算机内存 7.4 Intel处理器 7.5 汇编语言基础 7.6 用gdb调试 7.7 摘要 第8章 基本Linux攻击 8.1 栈操作 8.2 缓冲区溢出 8.3 本地缓冲区溢出攻击 8.4 远程缓冲器溢出攻击 8.5 摘要 第9章 高级Linux攻击 第10章 编写Linux Shellcode 第11章 编写基本的Windows攻击第4部分 漏洞分析 第12章 被动分析 第13章 高级逆向工程 第14章 从发现漏洞到攻击漏洞 第15章 关闭漏洞：缓解

版权说明