

《黑客秘笈》

图书基本信息

书名：《黑客秘笈》

13位ISBN编号：9787115393680

出版时间：2015-7-1

作者：[美]彼得·基姆

页数：196

译者：徐文博,成明遥

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《黑客秘笈》

内容概要

所谓的渗透测试，就是借助各种漏洞扫描工具，通过模拟黑客的攻击方法，来对网络安全进行评估。本书采用大量真实案例和集邮帮助的建议讲解了在渗透测试期间会面临的一些障碍，以及相应的解决方法。本书共分为10章，其内容涵盖了本书所涉的攻击机器/工具的安装配置，网络扫描，漏洞利用，人工地查找和搜索Web应用程序的漏洞，攻陷系统后如何获取更重要的信息，社工方面的技巧，物理访问攻击，规避杀毒软件的方法，破解密码相关的小技巧和最终的成果汇总等知识。

本书编排有序，章节直接相互独立，读者可以按需阅读，也可以逐章阅读。本书不要求读者具备渗透测试的相关背景，但是如果具有相关的经验，对理解本书的内容会更有帮助。

《黑客秘笈》

作者简介

Peter Kim是Secure Planet公司的CEO兼主席，在安全领域具有近10年的从业经验，在过去的7年里，一直从事渗透测试工作。他曾经在马里兰州霍华德社区学院讲授过渗透测试和网络安全的课程，并且持有大量安全相关的认证。

书籍目录

- 1.1 搭建渗透测试主机
 - 1.1.1 硬件规格
 - 1.1.2 商业软件
 - 1.1.3 Kali Linux (<http://www.kali.org>)
 - 1.1.4 Windows虚拟机
- 1.2 总结
- 第2章 发球前—扫描网络
 - 2.1 外部扫描
 - 2.2 Discover Scripts (过去叫做Backtrack Scripts) (Kali Linux)
 - 2.2.1 被动式信息收集的操作方法
 - 2.2.2 使用泄漏库来查找邮箱、认证信息
 - 2.3 外部或内部的主动式信息收集
 - 2.4 Web应用程序的扫描
 - 2.4.1 Web应用程序的扫描流程
 - 2.4.2 Web应用程序的扫描工具
 - 2.5 总结
- 第3章 带球—漏洞利用
 - 3.1 Metasploit (Windows/Kali Linux) (<http://www.metasploit.com>)
 - 3.1.1 配置Metasploit进行远程攻击的基本步骤
 - 3.1.2 搜索Metasploit的exploit (以古老的MS08-067漏洞为例)
 - 3.2 脚本
 - 3.3 总结
- 第4章 抛传—Web应用程序的人工检测技术
 - 4.1 Web应用程序的渗透测试
 - 4.1.1 SQL注入
 - 4.1.2 跨站脚本 (XSS)
 - 4.1.3 跨站请求伪造 (CSRF)
 - 4.1.4 会话令牌
 - 4.1.5 模糊测试/输入验证
 - 4.1.6 功能/业务逻辑测试
 - 4.2 总结
- 第5章 横传—渗透内网
 - 5.1 无登录凭据条件下的网络渗透
 - 5.2 利用任意域凭据 (非管理权限)
 - 5.2.1 组策略首选项
 - 5.2.2 获取明文凭据
 - 5.2.3 关于漏洞利用后期的一点提示
 - 5.3 利用本地或域管理账号
 - 5.3.1 使用登录凭据和PSEXEC掌控网络
 - 5.3.2 攻击域控制器
 - 5.4 漏洞利用的后期阶段—使用PowerSploit (Windows)
 - 5.5 漏洞利用的后期阶段—PowerShell篇 (Windows)
 - 5.6 ARP欺骗
 - 5.6.1 IPv4
 - 5.6.2 IPv6
 - 5.6.3 ARP欺骗之后的攻击步骤
 - 5.6.4 会话劫持 (SideJacking)

5.6.5 Hamster/Ferret (Kali Linux)

5.7 端口代理

5.8 总结

第6章 助攻—社会工程学

6.1 近似域名

6.1.1 SMTP攻击

6.1.2 SSH攻击

6.2 鱼叉式网络钓鱼

6.2.1 Metasploit Pro 的网络钓鱼模块

6.2.2 社会工程学工具集 (Kali Linux)

6.2.3 大规模鱼叉式网络钓鱼

6.2.4 Excel相关的社会工程学

6.3 总结

第7章 短传—需要物理访问的攻击

7.1 无线攻击

7.1.1 被动识别和侦察

7.1.2 主动攻击

7.2 物理攻击

7.2.1 克隆工卡

7.2.2 渗透测试便携设备

7.2.3 物理社会工程学攻击

7.3 总结

第8章 四分卫突破—规避反病毒检测

8.1 规避反病毒检测

8.1.1 在反病毒扫描中隐藏Windows Credential Editor
(基于Windows平台)

8.1.2 Python

8.2 总结

第9章 特勤组—破解、利用和技巧

9.1 密码破解

9.1.1 John The Ripper (JTR)

9.1.2 oclHashcat

9.2 漏洞搜索

9.2.1 Searchsploit (Kali Linux)

9.2.2 BugTraq

9.2.3 Exploit-DB

9.2.4 查询Metasploit

9.3 一些小技巧

9.3.1 Metasploit中的RC脚本

9.3.2 绕过UAC

9.3.3 绕过域名的Web过滤

9.3.4 Windows XP—古老的FTP策略

9.3.5 隐藏文件 (Windows)

9.3.6 保持隐藏文件 (Windows)

9.3.7 上传文件到Windows 7/8主机

第10章 赛后—分析报告

第11章 继续教育

11.1 重要会议

11.2 培训课程

11.3 书籍

11.4 漏洞渗透测试框架

11.5 夺旗 (CTF)

11.6 与时俱进

最后的注意事项

致谢

《黑客秘笈》

精彩短评

- 1、 战术流程 有很多挺有意思的资源
- 2、 只是简单罗列一下 有哪些工具 没有价值的书
- 3、 现在的黑客都沦为只会用工具了

《黑客秘笈》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com