

《黑客攻防实战详解》

图书基本信息

书名：《黑客攻防实战详解》

13位ISBN编号：9787121022210

10位ISBN编号：7121022214

出版时间：2006年03月

出版社：电子工业出版社

作者：邓吉

页数：474 页

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.tushu111.com

《黑客攻防实战详解》

内容概要

《黑客攻防实战详解》是《黑客攻防实战入门》的姊妹篇，从“攻”、“防”两个不同的角度，通过现实中的入侵实例，并结合作者的心得体会，图文并茂地再现了网络入侵与防御的全过程。《黑客攻防实战详解》共分3篇共11章，系统地介绍了入侵的全部过程，以及相应的防御措施和方法。其中包括信息的搜集、基于认证的入侵及防御、基于漏洞的入侵及防御、基于木马的入侵及防御、入侵中的隐藏技术、入侵后的留后门以及清脚印技术。《黑客攻防实战详解》用图解的方式对每一个入侵步骤都进行了详细的分析，以推测入侵者的入侵目的；对入侵过程中常见的问题进行了必要的说明与解答；并对一些常见的入侵手段进行了比较与分析，以方便读者了解入侵者常用的方式、方法，保卫网络安全。

《黑客攻防实战详解》适合于网络技术爱好者、网络系统管理员阅读，及可作为相关专业学生的学习资料和参考资料。

书籍目录

- 第1篇 入门篇第1章 一次完整的入侵
 - 21.1 搭建局域网
 - 21.2 认识扫描器
 - 71.3 一次完整的入侵
 - 91.4 小结
- 23第2章 信息搜集
 - 242.1 网站信息搜集
 - 242.1.1 相关知识
 - 242.1.2 信息搜集
 - 272.1.3 网站注册信息搜集
 - 302.1.4 结构探测
 - 342.1.5 搜索引擎
 - 382.2 资源搜集
 - 392.2.1 共享资源简介
 - 392.2.2 共享资源搜索
 - 402.2.3 破解Windows 9x共享密码
 - 422.2.4 利用共享资源入侵
 - 432.2.5 FTP资源扫描
 - 442.2.6 安全解决方案
 - 452.2.7 常见问题与解答
 - 452.3 端口扫描
 - 462.3.1 网络基础知识
 - 462.3.2 端口扫描原理
 - 492.3.3 端口扫描应用
 - 492.3.4 操作系统识别
 - 522.3.5 常见问题与解答
 - 522.4 综合扫描
 - 532.4.1 X-Scan
 - 532.4.2 流光Fluxay
 - 582.4.3 X-WAY
 - 612.4.4 扫描器综合性能比较
 - 642.4.5 常见问题与解答
 - 642.5 小结
- 65第2篇 基础篇第3章 基于认证的入侵
 - 683.1 获取账号密码
 - 683.1.1 弱口令扫描
 - 683.1.2 字典攻击
 - 703.1.3 暴力破解
 - 743.1.4 网络监听获取密码
 - 773.1.5 其他途径
 - 793.1.6 常见问题与解答
 - 813.2 IPC\$入侵
 - 823.2.1 IPC\$简介
 - 823.2.2 远程文件操作
 - 833.2.3 IPC\$空连接漏洞
 - 883.2.4 安全解决方案
 - 903.2.5 常见问题与解答

- 923.3 Telnet入侵
 - 933.3.1 Telnet简介
 - 933.3.2 Telnet典型入侵
 - 943.3.3 Telnet杀手锏
 - 983.3.4 Telnet高级入侵全攻略
 - 1013.3.5 常见问题与解答
- 1053.4 利用注册表入侵
 - 1053.4.1 注册表简介
 - 1063.4.2 远程开启及连接远程主机的“远程注册表服务”
 - 1073.4.3 编辑注册表(REG)文件
 - 1083.4.4 常用注册表入侵方法
- 1103.5 利用远程计算机管理入侵
 - 1133.5.1 计算机管理简介
 - 1133.5.2 开启远程计算机管理服务
 - 1143.5.3 管理远程计算机
 - 1173.5.4 利用远程控制软件对远程计算机进行入侵
 - 1203.5.5 常见问题与解答
- 1233.6 利用远程终端服务(3389)入侵
 - 1243.6.1 终端服务的概念
 - 1243.6.2 远程开启远程终端服务(3389)
 - 1243.6.3 使用远程终端服务入侵
 - 1273.6.4 常见问题与解答
- 1303.7 利用MS SQL入侵
 - 1303.7.1 利用MS SQL弱口令入侵
 - 1303.7.2 入侵MS SQL数据库
 - 1353.7.3 入侵MS SQL主机
 - 1353.7.4 利用SQL注入攻击
 - 1403.7.5 利用NBSI软件进行SQL注入攻击
- 1443.7.6 安全解决方案
- 1463.8 利用FTP入侵
 - 1473.8.1 FTP简介
 - 1473.8.2 利用FTP弱口令入侵
 - 1493.8.3 利用FTP匿名登录入侵
 - 1543.8.4 利用FTP提升本地权限
 - 1573.8.5 利用SlimFTP制作FTP肉鸡
 - 1583.8.6 安全解决方案
- 1603.9 远程命令执行及进程查杀
 - 1603.8.1 远程执行命令
 - 1603.9.2 查、杀进程
 - 1613.9.3 远程执行命令方法汇总
 - 1643.9.4 常见问题与解答
- 1643.10 小结
- 165第4章 基于服务器软件漏洞的入侵
 - 1664.1 IIS漏洞(一)
 - 1664.1.1 IIS基础知识
 - 1664.1.2 .ida&.idq漏洞
 - 1674.1.3 .printer漏洞
 - 1744.1.4 Unicode目录遍历漏洞
 - 1774.1.5 .asp映射分块编码漏洞

- 1874.2 IIS漏洞（二）
- 1894.2.1 WebDAV远程缓冲区溢出漏洞
- 1894.2.2 WebDAV超长请求远程拒绝服务攻击漏洞
- 1944.2.3 WebDAV XML消息处理远程拒绝服务漏洞
- 1964.2.4 Windows Media服务nsiislog.dll远程缓冲区溢出漏洞
- 2004.2.5 Microsoft FrontPage Server Extensions远程缓冲区溢出漏洞
- 2054.2.6 常见问题与解答
- 2084.3 论坛漏洞
- 2084.3.1 上传漏洞
- 2084.3.2 暴库漏洞
- 2184.3.3 常见问题与解答
- 2314.4 Blog漏洞
- 2314.4.1 直接下载数据库漏洞
- 2314.4.2 Cookie欺骗漏洞
- 2464.4.3 常见问题与解答
- 2544.5 Serv-U漏洞（一）
- 2544.5.1 Serv-U FTP服务器MDTM命令远程缓冲区溢出漏洞
- 2554.5.2 Serv-U本地权限提升漏洞
- 2614.5.3 常见问题与解答
- 2654.6 小结
- 265第5章 Windows操作系统漏洞
- 2665.1 本地提权类漏洞
- 2665.1.1 Microsoft Windows内核消息处理本地缓冲区溢出漏洞
- 2665.1.2 Microsoft Windows LPC本地堆溢出漏洞
- 2705.1.3 Microsoft OLE和COM远程缓冲区溢出漏洞
- 2725.2 用户交互类漏洞
- 2755.2.1 Microsoft Task Scheduler远程任意代码执行漏洞
- 2755.2.2 Microsoft Windows GDI+ JPG解析组件缓冲区溢出漏洞
- 2775.2.3 Microsoft Windows图形渲染引擎安全漏洞
- 2835.2.4 Microsoft压缩文件夹远程任意命令执行漏洞
- 2865.2.5 Microsoft Windows ANI文件解析远程缓冲区溢出漏洞
- 2885.2.6 Microsoft Windows MSHTA脚本执行漏洞
- 2915.3 远程溢出漏洞
- 2985.3.1 Microsoft UPnP存在缓冲溢出漏洞
- 2985.3.2 Microsoft RPC接口远程任意代码可执行漏洞
- 3005.3.3 Microsoft Windows Messenger服务远程堆溢出漏洞
- 3055.3.4 Windows ASN_1库BER解码堆破坏漏洞
- 3085.3.5 Windows Local Security Authority Service远程缓冲区溢出漏洞
- 3135.3.6 Microsoft WINS服务远程缓冲区溢出漏洞
- 3175.3.7 Microsoft Windows即插即用功能远程缓冲区溢出漏洞
- 3205.4 小结
- 324第6章 基于木马的入侵
- 3256.1 木马的工作原理
- 3266.1.1 木马是如何工作的
- 3266.1.2 木马的隐藏
- 3266.1.3 木马是如何启动的
- 3286.1.4 黑客如何欺骗用户运行木马
- 3306.2 木马的种类
- 3316.3 木马的演变

- 3336.4 第二代木马
 - 3336.4.1 冰河
 - 3336.4.2 广外女生
- 3396.5 第三代与第四代木马
 - 3436.5.1 木马连接方式
 - 3436.5.2 第三代木马——灰鸽子
 - 3456.5.3 第四代木马
 - 3486.5.4 常见问题与解答
- 3556.6 第五代木马
- 3556.7 木马防杀技术
 - 3566.7.1 加壳与脱壳
 - 3566.7.2 木马防杀实例
- 3576.8 种植木马
 - 3596.8.1 修改图标
 - 3596.8.2 文件合并
 - 3606.8.3 文件夹木马
 - 3626.8.4 网页木马
 - 3646.8.5 CHM电子书木马
- 3676.9 安全解决方案
- 3696.10 常见木马的手动清除
 - 3706.10.1 冰河木马
 - 3706.10.2 ShareQQ木马
 - 3706.10.3 BladeRunner木马
 - 3716.10.4 广外女生
 - 3716.10.5 BrainSpy木马
 - 3716.10.6 FunnyFlash木马
 - 3716.10.7 QQ密码侦探特别版木马
 - 3726.10.8 IEthief木马
 - 3726.10.9 QEyes潜伏者
 - 3726.10.10 蓝色火焰
 - 3726.10.11 Back Construction木马
- 3736.11 常见问题与解答
- 3736.12 小结
- 373第7章 隐藏技术
 - 3747.1 文件传输与文件隐藏技术
 - 3747.1.1 IPC\$文件传输
 - 3747.1.2 FTP传输
 - 3757.1.3 打包传输
 - 3757.1.4 文件隐藏
 - 3787.1.5 常见问题与解答
 - 3817.2 扫描隐藏技术
 - 3817.2.1 流光Sensor
 - 3847.2.2 其他工具
 - 3877.2.3 常见问题与解答
 - 3877.3 入侵隐藏技术
 - 3887.3.1 跳板技术简介
 - 3887.3.2 手工制作跳板
 - 3887.3.3 Sock5代理跳板
 - 3947.3.4 端口重定向

- 4037.4 小结
- 405第8章 留后门与清脚印
 - 4068.1 账号后门
 - 4068.1.1 手工克隆账号
 - 4078.1.2 命令行方式下制作后门账号
 - 4128.1.3 克隆账号工具
 - 4168.1.4 常见问题与解答
 - 4208.2 漏洞后门
 - 4208.2.1 制造Unicode漏洞
 - 4208.2.2 制造.idq漏洞
 - 4228.3 木马后门
 - 4228.3.1 wolf
 - 4228.3.2 Winshell与WinEggDrop
 - 4288.3.3 SQL后门
 - 4298.4 清除日志
 - 4318.4.1 手工清除日志
 - 4318.4.2 通过工具清除事件日志
 - 4318.4.3 清除WWW和FTP日志
 - 4348.5 小结
- 435第9章 本地入侵
 - 4369.1 基础知识
 - 4369.2 盘载操作系统简介
 - 4369.3 ERD Commander
 - 4379.3.1 ERD Commander简介
 - 4379.3.2 利用ERD Commander进行入侵的实例
 - 4379.4 Windows PE
 - 4439.4.1 Windows PE简介
 - 4439.4.2 利用Windows PE入侵本地主机的三个实例
 - 4439.5 安全解决方案
 - 4499.6 本章小结
- 450第3篇 提高篇第10章 防火墙技术
 - 45210.1 防火墙概述
 - 45210.1.1 防火墙的定义
 - 45210.1.2 防火墙的规则
 - 45210.1.3 防火墙的功能
 - 45210.1.4 使用防火墙的好处
 - 45210.2 防火墙的分类
 - 45310.2.1 按实现方式分类
 - 45310.2.2 软件防火墙
 - 45310.2.3 硬件防火墙
 - 45310.2.4 按实现技术分类
 - 45310.2.5 数据包过滤防火墙
 - 45310.2.6 三应用级网关
 - 45510.2.7 状态包检测防火墙
 - 45610.3 常见防火墙简介
 - 45710.4 防火墙的结构
 - 45810.4.1 常见术语
 - 45810.4.2 双宿主机体系结构
 - 45810.4.3 被屏蔽主机体系结构

- 45910.4.4 被屏蔽子网体系结构
 - 45910.5 防火墙发现技术
 - 46010.5.1 黑客入侵带防火墙的操作系统的一般过程
 - 46010.5.2 跟踪技术
 - 46010.5.3 防火墙识别技术
 - 46010.5.4 路由跟踪
 - 46110.5.5 端口扫描
 - 46110.5.6 旗标攫取
 - 46110.5.7 防火墙审查技术
 - 46210.6 穿越防火墙技术
 - 46210.6.1 ICMP协议隧道
 - 46210.6.2 HTTP协议隧道
 - 46310.7 小结
 - 463第11章 BAT编程
 - 46411.1 批处理命令简介
 - 46411.2 在批处理文件中使用参数与组合命令
 - 46911.2.1 在批处理文件中使用参数
 - 46911.2.2 组合命令
 - 47011.3 管道命令
 - 47111.4 综合利用的实例
 - 47311.4.1 系统加固
 - 47311.4.2 删除日志
 - 47311.5 小结
- 474

精彩短评

- 1、 那是一个天真的时代.....
- 2、 那些自以为是的高手值得一看

章节试读

1、《黑客攻防实战详解》的笔记-第2页

配套视频是用"屏幕录像专家"录的.没有配音,纯打字.用的是微软拼音输入法,在记事本里面一直打字.第一个视频文件小红伞报警,这是第二个.

《黑客攻防实战详解》

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.tushu111.com