<<电脑硬道理-网络安全秘技>>

图书基本信息

书名：<<电脑硬道理-网络安全秘技>>

13位ISBN编号：9787894763280

10位ISBN编号：7894763284

出版时间：2010-5

出版时间：电脑报 电脑报电子音像出版社 (2010-05出版)

作者：电脑报 编

页数：326

<<电脑硬道理-网络安全秘技>>

内容概要

本手册正是一本了解黑客人侵，保卫信息财富的安全攻略，我们将常见的黑客人侵分为4个部分来讲解：第一篇主要介绍操作系统和局域网中容易被人忽视的安全问题；第二篇主要研究木马的本质并帮助你揪出电脑中的”内鬼“；第三篇涉及网站服务器的一些攻防，作为网管员应该了解并做好安全防范；第四篇属于综合案例篇，该篇融合了前面各部分基础内容，综合地揭露黑客的各种花招。
本手册几乎涵盖了网络安全的各个领域，详尽地为你揭露黑客神秘面纱，适合网络爱好者及网络管理员参考。

<<电脑硬道理-网络安全秘技>>

书籍目录

网络安全基础篇第1章 防黑防毒的认知与观念1.1 Internet世界的基本原理1.1.1 电脑的身份证——IP地址1.1.2 动态的IP地址1.1.3 端口扮演的角色与功能1.1.4 如何决定端口号码1.1.5 你的电脑打开了哪些端口1.2 黑客入侵电脑的目的1.2.1 个人电脑对黑客的利用价值1.2.2 黑客对网站或服务器的威胁1.2.3 小心你的通信被黑客截取1.3 黑客入侵电脑的方式1.3.1 入侵方式与防范1.3.2 黑客入侵的大致流程第2章 搭建安全测试环境2.1 开辟一块免杀区2.1.1 优化杀毒软件的配置2.1.2 还原杀毒软件隔离的程序2.1.3 注意自身系统安全2.1.4 放行测试程序2.2 虚拟黑客攻防环境2.2.1 配置虚拟机环境2.2.2 安装虚拟操作系统2.2.3 访问本机资源2.2.4.VMware也能“ Ghost ”2.2.5 组建一个虚拟网络2.2.6 用VMware组建虚拟网络环境2.3 搭建虚拟机网站平台2.3.1 搭建ASP网站平台2.3.2 搭建PHP脚本运行环境2.4 影子系统让本机更安全2.4.1 影子系统的介绍2.4.2 影子系统的操作2.5 安装配置沙盘软件2.5.1 Sandboxie的保护方式2.5.2 让Sanddboxie保护我们系统2.5.3 Sandboxie的其他设置第3章 踩点与侦查目标3.1 IP地址的扫描与防范3.1.1 容易被IP入侵的目标3.1.2 通过IP查找地理位置3.2 扫描网络资源3.2.1 搜索目标的扫描器3.2.2 搜索局域网中的活动主机3.2.3 查找局域网中的共享资源3.2.4 扫描目标主机开启的端口3.3 系统端口扫描利器——SuperScan3.3.1 获取目标IP地址3.3.2 使用SuperScarl的Ping功能3.3.3 利用SuperScarl检测端口3.4 扫描系统漏洞的X-Scan3.4.1 如何设定X.Scan的选项3.4.2 扫描及结果分析3.5 拥有密码破解功能的流光3.5.1 使用流光扫描目标主机3.5.2 分析扫描报告3.5.3 字典文件的密码破解3.6 防范黑客扫描3.6.1 关闭闲置和有潜在危险的端口3.6.2 用好防火墙第4章 Windows系统漏洞之攻防4.1 端口139——黑客入侵Windows的重要通道4.1.1 端口139的安全隐患4.1.2入侵端口139流程4.1.3 空连接漏洞4.1.4 防范端口139入侵4.2 警惕你的系统有后门4.2.1 不为人知的隐藏共享4.2.2 扫描出漏洞主机和账号4.2.3 连接漏洞主机4.2.4 留下后门账号4.2.5 IPC$连接WindowsXP4.2.6 关闭通道防范黑客入侵4.3 控制——黑客入侵的最高境界4.3.1 系统自带的远程利器4.3.2 登录远程电脑4.3.3 远程控制对方电脑4.3.4 防范黑客远程控制4.4 缓冲区溢出漏洞攻防4.4.1 什么是缓冲区溢出漏洞4.4.2 分析MS08.067远程溢出漏洞4.4.3 MS08.067远程溢出漏洞攻防4.4.4 MS04011缓冲区溢出实例4.4.5 通用批量溢出工具4.4.6 Wirldows蓝屏漏洞揭秘第5章 盗取局域网信息的嗅探器5.1 嗅探器如何截取信息5.1.1 嗅探器应用范围5.1.2 嗅探的前提条件5.1.3 共享式窃听5.1.4 交换式窃听5.2 嗅探器的类型5.2.1 嗅探器的特性的特性5.2.2 嗅探器分类5.3 小巧易用的Iris嗅探器5.3.1 s的特点5.3.2 设置与使用Iris5.3.3 利用s捕获邮箱密码5.3.4 利用s捕获relrlet会话密码5.4 网络间谍SpyNetSniffer5.4.1 SpyNetSrrifler设置5.4.2 使用SpyNetSniffer5.5 艾菲网页侦探5.5.1 艾菲网页侦探设置5.5.2 使用艾菲网页侦探木马攻防篇第6章 走进木马世界6.1 了解形形色色的木马6.1.1 什么是木马6.1.2 木马与病毒不同之处6.1.3 不同类型的木马6.2 C／S型木马的鼻祖——冰河6.2 11冰河的服务端配置6.2.2 远程控制服务端6.2.3 对冰河入侵的反击6.3 C／S型木马的经典——灰鸽子6.3.1 什么是反弹式木马6.3.2 反弹式木马灰鸽子的配置6.3.3 灰鸽子木马的强大破坏力6.3.4 FTP反弹式连接6.3.5 域名反弹连接6.3.6 客户端位于内网的配置方案6.4 用IE就能远控的B／S型木马——rmtsvc6.4.1 rmtsvc服务端的配置6.4.2 用浏览器控制远程电脑6.5 携带木马的下载者6.5.1 下载者木马的演示6.5.2 下载者使用的技巧6.5.3 短小精干的“ 一句话木马 ”第7章 火眼晶晶识木马7.1 小心下载文件有木马7.1.1 普通的文件捆绑7.1.2 捆绑到压缩文件中7.1.3 将木马植入到文件内部7.1.4 Ghost也可能被插入木马7.2 伪装文件的属性7.2.1 伪装属性信息7.2.2 伪装签名信息7.2.3 自定义签名7.3 文件图标的伪装7.3.1 生成图标7.3.2 替换图标7.4 通过网页夹带木马7.4.1 制作网页木马7.4.2 网站系统漏洞挂马法7.4.3 IIS写权限挂马法7.4.4 电子邮件挂马法7.5 视频文件挂马7.5.1 RM文件的伪装利用7.5.2 WMV文件的伪装利用7.6 Windows端口入侵挂马7.6.1 利用系统服务挂马7.6.2 利用网路服务挂马7.7 缓冲区溢出漏洞挂马7.7.1 黑客为何钟情数据溢出7.7.2专业工具入侵7.7.3 手工批量入侵7.7.4 工具批量入侵第8章 网页挂马与欺骗8.1 木马借框架网页隐身8.1.1 网页挂马的由来8.1.2 什么是IFRAME框架挂马8.1.3 IFRAME框架挂马实例分析8.2 借JS脚本偷偷挂木马8.2.1 JS挂马溯源8.2.2 JS挂马实例8.2.3 防范JS挂马8.3 为何信任网站有木马8.3.1 CSS挂马现象8.3.2 为什么会有CSS挂马8.3.3 CSS挂马实例8.3.4 防范CSS被挂马8.4 网页图片中潜伏的木马8.4.1 备受黑客青睐的图片挂马8.4.2 图片挂马攻防实例8.5 播放Flash招来木马8.5.1 SWF挂马优势8.5.2 SWF挂马攻防实例8.6 网页木马加密避追杀8.6.1 网页木马为什么要加密8.6.2 加密网页木马加密8.6.3 防范网页木马加密8.7 猫扑网的欺骗漏洞实例8.7.1 未过滤外部网址8.7.2钓鱼攻击演示8.7.3 网页挂马演示8.7.4 漏洞修补之法8.8 博客大巴网页漏洞引木马实例8.8.1

外部链接过滤不严8.8.2 博客大巴挂马揭秘8.8.3 再现跨站攻击第9章 木马与杀毒软件的角逐9.1 杀毒软件如何杀毒9.1.1 杀毒的原理9.1.2 基于文件扫描的技术9.1.3 认识了解PE文件结构9.1.4 认识并了解汇编语言9.2 修改特征码瞒骗杀毒软件9.2.1 设置MYCCL.复合特征码定位器9.2.2 划分特征码范围9.2.3 缩小特征码范围9.2.4 修改特征码内容9.2.5 特征码防杀总结9.3 加壳木马防范查杀9.3.1 壳是用来干什么的9.3.2 单一加壳伪装木马9.3.3 多重加壳伪装木马9.3.4 测试加壳木马9.3.5 利用加壳伪装木马的总结9.4 使用花指令防杀毒软件查杀9.4.1 什么是花指令9.4.2 垃圾代码是如何弄“ 晕 ”杀软件的9.4.3 揭秘花指令免杀步骤9.5 突破主动防御的手段9.5.1 什么是主动防御9.5.2 突破卡巴的主动防御9.5.3 其他杀毒软件主动防御9.5.4 木马程序自定义设置9.5.5 简单设置过主动防御9.5.6 捆绑程序过主动防御……第10章 服务器攻击与防范第11章 网站漏洞入侵与防范综合案例篇第12章 网游盗号与防范实例第13章 QQ攻击与防范实例第14章 电子邮箱攻防实例第15章 远程控制攻防实例第16章 行踪隐藏与痕迹清理第17章 密码破解与防范第18章 数据加密与解密附录 常用网络命令详解

章节摘录

插图：

编辑推荐

《电脑硬道理:网络安全秘技(第11版)》内容通俗易懂，语言风趣幽默，实例图文教学，理论实践结合，网络钓鱼、木马，诈骗，盗号……为你全面讲述各种黑客事件的来龙去脉，保卫我们的信息财富，安全平台软件，扫描嗅探工具，修改伪装工具，远程控制软件。
从何入门到精通网络爱好者入门首选指导手册丛书连续11年再版畅销260万册

版权说明