<<针锋相对>>

图书基本信息

书名：<<针锋相对>>

13位ISBN编号：9787111273127

10位ISBN编号：7111273125

出版时间：2009-7

出版时间：武新华、李防、 陈艳艳 机械工业出版社 (2009-07出版)

作者：武新华 等 著

页数：392

前言

神秘的黑客既让人害怕，又让人着迷。
在互联网技术飞速普及的今天，多了解一点黑客的入侵伎俩，学一点反黑客技术已成了行走网络江湖必备的防身术。
到底黑客世界是怎样的?黑客们通常使用什么技术、哪些工具来攻击目标?更为重要的是，我们应该如何来防范黑客的攻击。
本书作者根据多年的网络防御经验，在系统地总结网络中被广泛使用的入侵、防御技术的基础上，针对广大网管以及对网络爱好者的需求编写了此书。
希望能够有助于大家从多个角度了解网络安全技术，从而更有效地保护网络安全。
本书以深入剖析入侵过程为主线，向读者剖析了黑客如何实现信息的搜集；如何通过获取的信息打开目标服务器的切入点(基于身份验证、漏洞、木马的入侵)；如何实现远程连接；入侵后如何执行各种任务；如何留下后门，以便再次进入系统；以及黑客如何清除系统日志防止目标服务器发现入侵痕迹。
此外，书中还详细地介绍入侵者是如何实现从信息扫描到入侵过程中的隐身保护，如何逃避被他人发现。
本书对每一个入侵步骤作了详细的分析，以推断入侵者每一个入侵步骤的目的以及所要完成的任务，并对入侵过程中常见的问题作必要的说明与解答。
此外，本书还对几种常见的入侵手段进行了比较与分析。
本书主要通过介绍黑客攻击方式和工具，使读者了解黑客入侵的关键技术与方法，进而提高安全防护意识。
此外，本书还从黑客入侵防护应用角度给出了相对独立内容的论述，使读者对建构黑客入侵防范体系有一个基本概念和思路，为读者的安全防护系统建设方案提供一些有益的参考和借鉴。
本书的编写具有以下特色：·从零起步，通俗易懂，由浅入深地讲解，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客防范技巧与工具的使用方法。
·注重实用性，理论和实例相结合，并配以大量插图和配套光盘视频讲解，力图使读者能够融会贯通。
·介绍大量小技巧和小窍门，提高读者的工作效率，节省宝贵的摸索时间。
·重点突出、操作简练、内容丰富，同时附有大量的操作实例，读者可以一边学习，一边上机操作，做到即学即用、即用即得，让读者快速掌握。
本书采用通俗易懂的图文解说，易于上手；任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法；黑客技术盘点，让您实现“先下手为强”；攻防互参的防御方法，全面确保网络的安全。
参与本书编写的人员有武新华、李防、陈艳艳、李秋菊、张克歌、刘岩、段玲华、杨平等。
本书在编写过程中得到了许多热心网友的支持，参考了大量来自网络的资料，并对这些资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢。

内容概要

《针锋相对:黑客攻防实战揭秘》紧紧围绕黑客攻防技巧与工具的主题，深入浅出地剖析了用户在进行黑客防御时迫切需要用到的技术，使读者对网络防御技术有个系统了解，能够更好地防范黑客的攻击。

《针锋相对:黑客攻防实战揭秘》共分为11章，主要内容包括安全的测试环境、踩点侦察与漏洞扫描、Windows系统漏洞入侵防御、远程攻击与防御、常见漏洞扫描工具的使用、SQL的注入攻击与防御、留后门与清脚印技术、木马和间谍软件攻防实战、数据还原与恢复、系统进程与隐藏技术、系统清理与流氓软件清除等。

《针锋相对:黑客攻防实战揭秘》内容丰富、图文并茂、深入浅出，不仅适合作为广大网络爱好者的自学书籍，而且适合作为网络安全从业人员及网络管理员的参考用书。

书籍目录

前言第1章 安全的测试环境1．1黑客攻防基础知识1．1．1进程、端口和服务概述1．1．2DOS系统的常用命令1．1．3Windows注册表1．1．4Windows常用的服务配置1．2网络应用技术1．2．1TCP／IP协议簇1．2．2IP1．2．3ARP1．2．4ICMP1．3创建安全的测试环境1．3．1安全测试环境概述1．3．2虚拟机软件概述1．3．3用VMware创建虚拟环境1．3．4安装虚拟工具1．3．5在虚拟机中架设IIS服务器1．3．6在虚拟机中安装网站1．4可能出现的问题与解决方法1．5总结与经验积累第2章 踩点侦察与漏洞扫描2．1踩点与侦察范围2．1．1踩点概述2．1．2确定侦察范围2．1．3实施踩点的具体流程2．1．4网络侦察与快速确定漏洞范围2．1．5防御网络侦察与堵塞漏洞2．2确定扫描范围2．2．1确定目标主机的IP地址2．2．2确定可能开放的端口服务2．2．3确定扫描类型2．2．4常见的端口扫描工具2．2．5有效预防端口扫描2．3扫描服务与端口2．3．1获取NetBIOS信息2．3．2黑客字典2．3．3弱口令扫描工具2．3．4注入点扫描2．4可能出现的问题与解决方法2．5总结与经验积累第3章 Windows系统漏洞入侵防御3．1Windows服务器系统入侵流程3．1．1入侵Windows服务器的流程3．1．2NetBIOS漏洞攻防3．1．3IIS服务器攻防3．1．4缓冲区溢出攻防3．1．5用Serv-U创建FTP服务器3．2windows桌面用户系统防御3．2．1Windows-XP的账户登录口令3．2．2实现多文件捆绑3．2．3实现Windows系统文件保护3．2．4绕过Windows系统组策略3．3windows桌面用户网络攻防3．3．1JavaScript和ActiveX脚本攻防3．3．2XSS跨站点脚本攻防3．3．3跨Frame漏洞攻防3．3．4网络钓鱼攻防3．3．5蠕虫病毒攻防3．4Windows系统本地物理攻防3．4．1用盘载操作系统实施攻防3．4．3建立隐藏账户3．5Windows系统应用层攻防3．5．1窃取移动设备中的数据信息3．5．2查看星号密码3．5．3绕过防火墙3．5．4绕过查毒软件的保护3．6可能出现的问题与解决方法3．7总结与经验积累第4章 远程攻击与防御4．1远程攻击概述4．1．1远程攻击的分类4．1．2远程攻击的特点4．2局域网中的IP入侵4．2．1IP冲突攻击——网络特工4．2．2ARP欺骗攻击4．3QQ攻防4．3．1IP地址的探测4．3．2QQ炸弹攻防4．3．3进行远程控制的“QQ远控精灵”4．4DoS拒绝服务攻防4．4．1DoS攻击的概念和分类4．4．2DoS攻击常见的工具“4．4．3DoS攻击的防范措施4．5可能出现的问题与解决方法4．6总结与经验积累第5章 常见漏洞扫描工具的使用5．1常见的扫描工具5．1．1使用SSS扫描与防御5．1．2使用流光扫描5．2几款经典的网络嗅探器5．2．1用嗅探器SpyNetSniffer实现多种操作5．2．2能够捕获网页内容的艾菲网页侦探5．2．3局域网中的嗅探精灵IRIS5．3系统监控工具RealSpyMonitor5．4用pcAnywhere实现远程控制5．4．1安装pcAnywhere程序5．4．2设置pcAnywhere的性能5．4．3用pcAnywhere进行远程控制5．5可能出现的问题与解决方法5．6总结与经验积累第6章 SQL的注入攻击与防御6．1SQL的注入攻击6．1．1SQL注入攻击概述6．1．2实现SQL注入攻击6．1．3全面防御SQL注入攻击6．2尘缘雅境图文系统专用入侵工具6．3入侵SQL数据库6．3．1用MSSQL实现弱口令入侵6．3．2入侵MSSQL数据库6．3．3入侵MSSQL主机6．3．4辅助注入工具WIS6．3．5管理远程数据库6．3．6SAM数据库安全漏洞攻防6．4可能出现的问题与解决方法6．5总结与经验积累第7章 留后门与清脚印技术7．1后门技术的实际应用7．1．1手工克隆账号技术7．1．2程序克隆账号技术7．1．3制造Unicode漏洞后门7．1．4Wollf木马程序后门7．1．5在命令提示符中制作后门账号7．1．6SQL后门7．2清除登录服务器的日志信息7．2．1手工清除服务器日志7．2．2使用批处理清除远程主机日志7．2．3通过工具清除事件日志7．2．4清除WWW和FTP日志7．3清除日志工具的应用7．3．1日志清除工具elsave7．3．2日志清除工具CleanllSLog7．4可能出现的问题与解决方法7．5总结与经验积累第8章 木马和间谍软件攻防实战8．1木马的伪装8．1．1伪装成可执行文件8．1．2伪装成网页8．1．3伪装成图片木马8．1．4伪装成电子书木马8．2捆绑木马和反弹端口木马8．2．1熟悉木马的入侵原理8．2．2WinRAR捆绑木马8．2．3用网络精灵NetSpy实现远程监控8．2．4反弹端口型木马：网络神偷8．3反弹木马经典：灰鸽子8．3．1生成木马服务器8．3．2把木马植入到目标主机8．3．3预防被对方远程控制8．3．4手工清除“灰鸽子”8．4“冰河”木马的使用8．4．1配置“冰河”木马的被控端程序8．4．2搜索和远控目标主机8．4．3卸载和清除“冰河”木马8．5防不胜防的间谍软件8．5．1用spybot清理隐藏的间谍8．5．2间谍广告的杀手AD-Aware8．5．3反间谍软件8．6可能出现的问题与解决方法8．7总结与经验积累第9章 数据的还原与恢复9．1数据备份和补丁升级9．1．1数据备份9．1．2系统补丁的升级9．2恢复丢失的数据9．2．1数据恢复的

概念9．2．2 数据丢失的原因9．2．3 使用和维护硬盘时的注意事项9．2．4 数据恢复工具EasyRecovery9．2．5 恢复工具FinalData9．3 常用资料的备份和还原9．3．1 对操作系统进行备份和还原9．3．2 备份还原注册表9．3．3 备份还原IE收藏夹9．3．4 备份还原驱动程序9．3．5 备份还原数据库9．3．6 备份还原电子邮件9．4 可能出现的问题与解决方法9．5 总结与经验积累第10章 系统进程与隐藏技术10．1 恶意进程的追踪与清除10．1．1 系统进程和线程概述10．1．2 查看进程的发起程序10．1．3 查看、关闭和重建进程10．1．4 查看隐藏进程和远程进程10．1．5 查杀本机中的病毒进程10．2 文件传输与文件隐藏10．2．1 IPC$文件传输10．2．2 FTP传输与打包传输10．2．3 实现文件隐藏10．3 入侵隐藏技术10．3．1 代理服务器概述10．3．2 跳板技术概述10．3．3 手工制作跳板10．3．4 代理跳板10．4 可能出现的问题与解决方法10．5 总结与经验积累第11章 系统清理与流氓软件清除11．1 流氓软件的分类11．1．1 广告软件11．1．2 间谍软件11．1．3 浏览器劫持11．1．4 行为记录软件11．1．5 恶意共享软件11．2 金山系统清理专家11．2．1 查杀恶意软件11．2．2 在线系统诊断11．2．3 及时修补系统漏洞11．2．4 安全工具11．3 瑞星卡卡网络守护神11．3．1 常用的查杀工具11．3．2 七大保镖来护卫11．3．3 系统修复11．3．4 进程管理11．3．5 官方下载常用软件11．4 微软反间谍专家11．4．1 微软反间谍软件概述11．4．2 手动扫描查杀间谍软件11．4．3 设置定时自动扫描11．4．4 开启实时监控11．4．5 附带的特色安全工具11．5 奇虎360安全卫士11．5．1 清理恶评插件11．5．2 修复系统漏洞11．5．3 快速拥有安全软件11．5．4 免费查杀病毒11．6 诺盾网络安全特警11．6．1 系统安全风险提示与修复11．6．2 配置网络安全特警11．6．3 系统安全扫描11．6．4 身份安全登录设置11．6．5 其他功能11．7 可能出现的问题与解决11．8 总结与经验积累

章节摘录

插图：数据丢失的原因很多，如病毒、硬盘损坏等都会造成数据丢失，只有弄清楚数据丢失的源因才能为数据恢复找出对策。
造成数据丢失主要原因有以下几种：1．软件故障软件故障的类型主要包括受病毒感染、误格式化或误分区、误克隆、误删除或覆盖、黑客软件人为破坏、零磁道损坏、硬盘逻辑锁、操作时断电、意外电磁干扰造成数据丢失或破坏、系统错误或瘫痪造成文件丢失或破坏。
软件故障现象一般表现为：操作系统丢失、无法正常启动系统、磁盘读写错误、找不到所需要的文件、文件打不开、文件打开后乱码、硬盘没有分区、提示某个硬盘分区没有格式化等。
2．硬件故障硬件故障的类型主要包括磁盘划伤、磁头变形、磁臂断裂、磁头放大器损坏、芯片组或其他元器件损坏等。
硬件故障一般表现为系统无法识别硬盘，常有一种“咔嚓咔嚓”的磁组撞击声或电动机不转、通电后无任何声音、磁头定位不准造成读写错误等现象。

编辑推荐

《针锋相对:黑客攻防实战揭秘》为网络安全技术应用丛书之一。
安全的测试环境踩点侦查与漏洞扫描windows系统漏洞入侵防御远程攻击与防御常见漏洞扫描工具的使用SQL的注入攻击与防御木马和间谍软件攻防实战数据的还原与恢复系统进程与隐藏技术从零起步，循序渐进，步步深入荟萃大量经典实例、技巧，实用性强理论结合实践，重点突出、可读性强

版权说明