第一图书网, tushu007.com

<<网络攻防技术教程>>

图书基本信息

书名：<<网络攻防技术教程>>

13位ISBN编号：9787307099562

10位ISBN编号：730709956X

出版时间：2008-6

出版时间：杜晔、张大伟、 范艳芳 武汉大学出版社 (2012-08出版)

作者：杜晔，张大伟，范艳芳 著

页数：348

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：http://www.tushu007.com

内容概要

《高等学校信息安全专业规划教材：网络攻防技术教程（第2版）》详细地介绍了计算机及网 络系统面临的威胁与黑客攻击方法，详尽、具体地披露了攻击技术的真相， 以及防范策略和技术实现措施。
全书理论联系实际，在每部分技术讨论之后，都有一套详细的实验方案对相关技术进行验证。
《高等学校信息安全专业规划教材：网络攻防技术教程（第2版）》共分四个部分，内容由浅入深，按照黑 客攻击通常采用的步骤进行组织，分技术专题进行讨论。
第一部分介绍了网 络攻防基础知识，以使读者建立起网络攻防的基本概念。
第二部分介绍信息 收集技术，即攻击前的“ 踩点 ”，包括网络嗅探和漏洞扫描技术。
第三部分 是本书的核心内容，介绍了代表性的网络攻击技术，以及针对性的防御技术 。
第四部分着重于防御技术，讨论了PKI网络安全协议和两种得到广泛应用 的安全设备，即防火墙和入侵检测系统。
《高等学校信息安全专业规划教材：网络攻防技术教程（第2版）》可作为信息安全、计算机、通信等专业 本科生、硕士研究生的教科书，也适合于网络管理人员、安全维护人员和相 关技术人员参考和阅读。

书籍目录

第一部分 网络攻击基础知识第1章 黑客与安全事件 1.1 网络安全事件 1.2 黑客与入侵者 1.2.1 黑客简史 1.2.2 黑客的定义 1.2.3 入侵者 1.3 黑客攻击目标与步骤 1.3.1 黑客攻击的目标 1.3.2 黑客攻击的步骤 1.4 黑客攻击发展趋势 1.5 社会工程学第2章 网络攻防相关概念 2.1 0SI安全体系结构 2.1.1 五类安全服务 2.1.2 安全服务提供的安全机制 2.1.3 安全服务和特定安全机制的关系 2.1.4 0SI安全体系的管理 2.2 网络脆弱性分析 2.2.1 网络安全威胁 2.2.2 网络安全风险 2.2.3 网络脆弱性 2.3 网络攻击的分类 2.4 主动攻击与被动攻击 2.4.1 主动攻击 2.4.2 被动攻击 2.5 网络安全模型 2.5.1 P2DR模型 2.5.2 PDR2模型第二部分 信息收集技术第3章 网络嗅探 3.1 嗅探器概述 3.1.1 嗅探器简介 3.1.2 嗅探器的工作原理 3.2 交换式网络上的嗅探 3.3 简易网络嗅探器的实现 3.4 嗅探器的检测与防范 3.5 常用嗅探工具 3.5.1 Tcpdump 3.5.2 Libpcap 3.5.3 SnifferPro 3.5.4 WireShark 实验部分 【实验3.1】 wireShark嗅探器的使用 【实验3.2】 snifferPro嗅探器的使用 【实验3.3】 Telnet协议密码嗅探第4章 漏洞扫描 4.1 系统漏洞 4.1.1 漏洞的概念 4.1.2 已知系统漏洞 4.2 漏洞扫描相关知识 4.2.1 漏洞扫描基本原理 4.2.2 漏洞扫描的分类 4.2.3 漏洞扫描器的组成 4.3 扫描策略与防范 4.3.1 端口扫描与防范 4.3.2 漏洞扫描与防范 4.4 常用扫描工具 实验部分 【实验4.1】 Ping命令的使用 【实验4.2】 Superscan工具的使用 【实验4.3】 Nmap工具的使用 【实验4.4】 综合扫描工具——流光Fluxay的使用第三部分 网络攻击技术第5章 拒绝服务攻击 5.1 拒绝服务攻击概述 5.1.1 什么是拒绝服务攻击 5.1.2 拒绝服务攻击原理 5.1.3 拒绝服务攻击时的现象 5.2 分布式拒绝服务攻击 5.2.1 分布式拒绝服务攻击背景 5.2.2 分布式拒绝服务攻击的步骤 5.2.3 分布式拒绝服务攻击分类 5.3 典型攻击与防范 5.4 DOS／DDoS攻击工具分析 实验部分 【实验5.1】 Misoskian ’sPacketBuilder攻击工具使用 【实验5.2】 阿拉丁uDP洪水攻击工具使用 【实验5.3】 独裁者Autocrat攻击工具使用第6章 缓冲区溢出攻击 6.1 缓冲区溢出攻击概述 6.1.1 什么是缓冲区溢出 6.1.2 缓冲区溢出攻击历史 6.1.3 缓冲区溢出原理 6.2 缓冲区溢出攻击分类 6.2.1 基于栈的缓冲区溢出 6.2.2 基于堆的缓冲区溢出 6.2.3 基于BSS段的缓冲区溢出 6.3 缓冲区溢出攻击的防范 6.3.1 编写正确的代码和代码审计 6.3.2 非执行的缓冲区 6.3.3 改进C语言函数库 6.3.4 数组边界检查 6.3.5 程序指针完整性检查 实验部分 【实验6.1】 Ms.06030本地权限提升 【实验6.2】 IIS5溢出工具使用 【实验6.3】 ida漏洞入侵第7章 Web应用安全攻击 7.1 Web应用安全概述 7.1.1 Web应用安全简介 7.1.2 Web应用相关技术 7.1.3 Web应用十大安全漏洞 7.2 SOL注入攻击 7.2.1 SQL注入的定义 7.2.2 SQL注入的原理 7.2.3 SSQL注入的实现过程 7.2.4 SQL注入的检测与防范 7.2.5 SQL注入提升权限攻击实例 7.3 跨站脚本攻击 7.3.1 跨站脚本攻击的定义 7.3.2 跨站脚本攻击的原理 7.3.3 跨站脚本攻击的实现过程 7.3.4 跨站脚本攻击的检测与防范 7.3.5 跨站脚本攻击实例分析 7.4 欺骗攻击 7.4.1 ARP欺骗网页劫持 7.4.2 DNS欺骗网站重定向 7.4.3 网络钓鱼 实验部分 【实验7.1】 “ 啊D ” SQL注入植入恶意程序 【实验7.2】 WlS和WEDSQL注入工具获取管理员权限 【实验7.3】 WinArpAttacker工具的使用第8章 病毒、蠕虫与木马 8.1 计算机病毒 8.1.1 计算机病毒的概念 8.1.2 计算机病毒的分类 8.1.3 计算机病毒的特点 8.1.4 计算机病毒的生命周期 8.1.5 典型病毒及其解决方案 8.2 蠕虫 8.2.1 蠕虫的概念 8.2.2 蠕虫的传播过程 8.2.3 与计算机病毒的区别 8.2.4 典型蠕虫与解决方案 8.3 木马 8.3.1 木马的概念 8.3.2 木马的分类 8.3.3 与计算机病毒的区别 8.3.4 木马植入手段 8.3.5 木马攻击原理 8.3.6 木马的查杀 8.3.7 典型木马与解决方案 实验部分 【实验8.1】 制作简单Word宏病毒 【实验8.2】 制作CHM木马 【实验8.3】 灰鸽子远程控制的配置第四部分 防御技术第9章 PKl网络安全协议 9.1 公钥基础设施PKI概述 9.1.1 PKI简介 9.1.2 PKI的组成 9.1.3 PKI的功能 9.2 公钥基础设施PKI的应用 9.2.1 基于PKI的服务 9.2.2 SSL协议 9.2.3 虚拟专用网VPN 9.2.4 安全电子邮件 9.2.5 Web安全 9.3 usBKey在PKI中的应用 9.3.1 USBKey简介 9.3.2 USBKey的特点 9.3.3 WindOWSCSP简介 实验部分 【实验9.1】 WindowsServer中CA的配置 【实验9.2】 配置SSL安全站点 【实验9.3】 使用USBKey申请客户证书 【实验9.4】 客户端使用USBKey登录SSL站点 【实验9.5】 使用USBKey签名和加密电子邮件第1O章 防火墙 10.1 防火墙技术概述 lO.1.1 防火墙的概念 10.1.2 防火墙的发展过程 lO.1.3 防火墙基本安全策略 10.1.4 防火墙的优点 10.2 防火墙系统的分类 10.2.1 按结构分类 10.2.2 按技术分类 10.3 防火墙关键技术 10.3.1 数据包过滤 lO.3.2 代理技术 lO.3.3 网络地址转换 10.3.4 身份认证技术 10.3.5 安全审计和报警 10.3.6 流量统计和控制 10.4 防火墙的发展方向 实验部分 【实验10.1】 天网防火墙的配置 【实验10.2】 添加天网防火墙规则，并验证效果第11章 入侵检测系统 11.1 入侵检测技术概述 11.1.1 入侵检测的概念

11.1.2 入侵检测的发展史 11.1.3 通用入侵检测系统结构 11.1.4 入侵检测系统标准化 11.2 入侵检测系统分类 11.2.1 数据来源 11.2.2 分析方法 11.2.3 时效性 11.2.4 分布性 11.3 入侵检测系统的分析技术 11.3.1 异常入侵检测技术 11.3.2 误用入侵检测技术 11.3.3 异常检测与误用检测评价 11.4 典型入侵检测系统 11.4.1 Snort系统 l1.4.2 DIDS系统 11.4.3 AAFID系统 11.4.4.EMERALD系统 11.4.5 NetSTAT系统 11.5 入侵检测系统的发展方向 实验部分 【实验11.1】 Snort系统的安装与配置 【实验11.2】 添加Snort规则，并验证检测效果 附录附录一 Sniffer程序源代码附录二 常用跨站脚本攻击方法参考文献

编辑推荐

杜晔等编著的《网络攻防技术教程(第2版）》的特点在于理论联系实际。
在技术讨论之后，都有一套详细的试验方案对相关技术进行验证。
通过具体的试验操作，帮助读者实际掌握和理解各个知识点的精髓。
考虑到不同单位千差万别的试验条件，我们的试验内容大部分基于很容易搭建的windows和Linux操作系统，充分降低了试验开设过程的成本。
　本书共分四个部分，内容由浅入深，按照黑客攻击通常采用的步骤进行组织，分技术专题进行讨论。
第一部分介绍了网络攻防基础知识，以使读者建立起网络攻防的基本概念。
第二部分介绍信息收集技术，即攻击前的“踩点”，包括网络嗅探和漏洞扫描技术。
第三部分是本书的核心内容，介绍了代表性的网络攻击技术，以及针对性的防御技术。
第四部分着重于防御技术，讨论了PKI网络安全协议和两种得到广泛应用的安全设备，即防火墙和入侵检测系统。

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:http://www.tushu007.com