

<<黑客攻防实战进阶>>

图书基本信息

书名：<<黑客攻防实战进阶>>

13位ISBN编号：9787121052828

10位ISBN编号：7121052822

出版时间：2008-1

出版时间：电子工业

作者：罗诗尧

页数：385

字数：595000

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>

<<黑客攻防实战进阶>>

内容概要

作为畅销书《黑客攻防实战入门》与《黑客攻防实战详解》的提高篇，本书分6章详细介绍了漏洞溢出入侵、Web攻击、网马与木马、路由器攻击、无线入侵、Nessus插件编程这些目前热门的黑客攻防高级知识和实战技巧，通过再现现实中发生的黑客攻防案例，不仅为读者耐心讲解“怎么做”，而且为读者剖析“为什么”。

本书可作为网络技术爱好者、网络系统管理员的参考用书，也可作为相关专业学生的指导教材。

<<黑客攻防实战进阶>>

书籍目录

第1章 漏洞溢出入侵	1.1 何为溢出型漏洞	1.1.1 缓冲区溢出漏洞利用历史	1.1.2 溢出原理
和本地溢出	1.1.3 远程溢出	1.1.4 溢出的高级利用	1.2 栈溢出漏洞的利用
中断地址	1.2.2 利用中断的覆盖	1.2.3 通用地址覆盖	1.2.4 覆盖异常
常的另一种利用方法	1.3 堆溢出漏洞	1.3.1 堆溢出概念	1.3.2 堆溢出实例
小结及防范	1.4.1 非执行的缓冲区	1.4.2 编写安全正确的代码	1.4.3 数组边界检查
1.4.4 程序指针完整性检查	1.4.5 程序指针完整性检查与数组边界检查的比较	1.4.6 一些具体的预防措施	1.4.7 普通用户防范缓冲区溢出的方法
Windows本地溢出实例	1.5.2 Windows远程溢出实例	1.5.3 强大的万能溢出工具MetasploitFramework 2.7	第2章 Web攻击
面的Web欺骗	2.1.3 基于程序的Web欺骗	2.2 SQL注入	2.1 Web欺骗攻击
一个简单的实例	2.2.3 用浏览器直接提交数据	2.2.1 测试环境的搭建	2.1.1 网络钓鱼
高级利用	2.2.6 对Very-Zone SQL注入漏洞的利用	2.2.4 注入漏洞的利用	2.1.2 基于面的Web欺骗
2.2.8 使用工具进行SQL注入	2.2.9 对SQL注入漏洞的防御	2.2.5 注入漏洞的高级利用	2.2 对动易商城2006 SQL注入漏洞的利用
站的来源	2.3.2 简单留言本的跨站漏洞	2.3 跨站脚本攻击	2.3.1 跨站漏洞的利用
站漏洞预防和防御	2.4 Web后门及加密隐藏	2.4.1 什么是Web后门	2.3.2 简单留言本的跨站漏洞
2.4.3 Web后门的隐藏	2.5 Web权限提升	2.5.1 系统漏洞提权	2.3.3 跨站漏洞的利用
权	2.5.3 配置不当提升系统权限(陷阱式提权)	2.6 Web服务器上的指纹鉴定	2.3.4 未雨绸缪——对跨站漏洞预防和防御
检测系统(I.D.S)	2.6.2 蜜罐技术	2.6.1 入侵检测系统(I.D.S)	2.4.2 Web后门免杀
木马免杀	3.1.3 网马隐藏	3.2 木马和后门	2.5.2 第三方软件权限提权
客的最爱Rootkit	3.2 木马和后门	3.2.1 赤兔马	2.5.3 配置不当提升系统权限(陷阱式提权)
第4章 路由器攻击	4.1 路由器介绍	4.1.1 什么是路由器	2.6.2 蜜罐技术
线器、交换机的区别	4.1.3 路由器的种类	4.2 ADSL家庭路由	3.1 网马
通过ADSL路由器入侵内网	4.3 入侵Cisco路由器	4.2.1 默认口令入侵	3.1.1 认识网马
置缺陷入侵Cisco路由器	5.1 无线威胁概述	5.1.1 什么是无线威胁	3.1.3 网马隐藏
无线网络基本知识	5.2 无线广播SSID	5.3 Wi-Fi功能漏洞	3.2 木马和后门
网络配置实例	5.6 LEAP	5.4 比较WEP与WPA	3.2.1 赤兔马
系结构与工作流程	6.3 Nessus安装与配置	6.1 Nessus简介	3.2.2 木马免杀
服务器端插件升级	6.3.3 Nessus服务器端基本配置	6.2 Nessus服务器端插件升级	3.2.3 木马免杀
用Nessus进行扫描	6.4.1 用Nessus服务器端进行扫描	6.3.1 Nessus服务器端下载与安装	3.3 网马隐藏
经典扫描案例	6.5 Nessus插件与脚本解释器	6.3.2 Nessus服务器端插件升级	4.1 路由器介绍
一个NASL插件	6.6 NASL插件编程入门实例	6.3.3 Nessus服务器端基本配置	4.1.1 什么是路由器
例	6.7.2 NASL脚本结构	6.3.4 Nessus客户端下载与安装	4.1.2 路由器与线器、交换机的区别
NASL重要函数:字符串处理函数	6.7.3 NASL语法	6.4 用Nessus进行扫描	4.2 ADSL家庭路由
本优化	6.7.4 NASL重要函数:网络相关函数	6.4.1 用Nessus服务器端进行扫描	4.2.1 默认口令入侵
6.9 编写自己的NASL插件	6.7.6 如何编写一个高效的Nessus安全测试插件	6.4.2 用Nessus客户端进行扫描	4.3 入侵Cisco路由器
检测TFTP服务器的目录遍历漏洞	6.7.7 脚本优化	6.4.3 经典扫描案例	4.3.1 Cisco路由器基础
6.10 NASL脚本的调试	6.8.1 检测FTP匿名登录	6.5 无线网络基本知识	4.3.2 SNMP配置缺陷入侵Cisco路由器
6.11 小结	6.8.2 检测是否运行TFTP服务	5.1 无线威胁概述	5.1 无线威胁概述
	6.9.1 检测一个FTP的拒绝服务漏洞(未曾公布过的漏洞)	5.1.1 什么是无线威胁	5.1.1 什么是无线威胁
	6.9.2 检测TFTP服务器的目录遍历漏洞	5.2 无线广播SSID	5.2 无线广播SSID
		5.3 Wi-Fi功能漏洞	5.3 Wi-Fi功能漏洞
		5.4 比较WEP与WPA	5.4 比较WEP与WPA
		5.5 无线网络配置实例	5.5 无线网络配置实例
		5.6 LEAP	5.6 LEAP
		5.7 攻陷WEP	5.7 攻陷WEP
		6.1 Nessus简介	6.1 Nessus简介
		6.2 Nessus服务器端插件升级	6.2 Nessus服务器端插件升级
		6.3.1 Nessus服务器端下载与安装	6.3.1 Nessus服务器端下载与安装
		6.3.2 Nessus服务器端基本配置	6.3.2 Nessus服务器端基本配置
		6.3.3 Nessus客户端下载与安装	6.3.3 Nessus客户端下载与安装
		6.4 用Nessus进行扫描	6.4 用Nessus进行扫描
		6.4.1 用Nessus服务器端进行扫描	6.4.1 用Nessus服务器端进行扫描
		6.4.2 用Nessus客户端进行扫描	6.4.2 用Nessus客户端进行扫描
		6.4.3 经典扫描案例	6.4.3 经典扫描案例
		6.5 Nessus插件与脚本解释器	6.5 Nessus插件与脚本解释器
		6.6 NASL插件编程入门实例	6.6 NASL插件编程入门实例
		6.6.1 编写第一个NASL插件	6.6.1 编写第一个NASL插件
		6.6.2 如何安装插件	6.6.2 如何安装插件
		6.7 Nessus插件开发语言——NASL	6.7 Nessus插件开发语言——NASL
		6.7.1 Hello World示例	6.7.1 Hello World示例
		6.7.2 NASL脚本结构	6.7.2 NASL脚本结构
		6.7.3 NASL语法	6.7.3 NASL语法
		6.7.4 NASL重要函数:网络相关函数	6.7.4 NASL重要函数:网络相关函数
		6.7.5 NASL重要函数:字符串处理函数	6.7.5 NASL重要函数:字符串处理函数
		6.7.6 如何编写一个高效的Nessus安全测试插件	6.7.6 如何编写一个高效的Nessus安全测试插件
		6.7.7 脚本优化	6.7.7 脚本优化
		6.8 NASL插件实例分析	6.8 NASL插件实例分析
		6.8.1 检测FTP匿名登录	6.8.1 检测FTP匿名登录
		6.8.2 检测是否运行TFTP服务	6.8.2 检测是否运行TFTP服务
		6.9 编写自己的NASL插件	6.9 编写自己的NASL插件
		6.9.1 检测一个FTP的拒绝服务漏洞(未曾公布过的漏洞)	6.9.1 检测一个FTP的拒绝服务漏洞(未曾公布过的漏洞)
		6.9.2 检测TFTP服务器的目录遍历漏洞	6.9.2 检测TFTP服务器的目录遍历漏洞
		6.10 NASL脚本的调试	6.10 NASL脚本的调试
		6.11 小结	6.11 小结

<<黑客攻防实战进阶>>

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>