<<黑客渗透>>

图书基本信息

书名:<<黑客渗透>>

13位ISBN编号:9787894620248

10位ISBN编号: 7894620246

出版时间:2009-4

出版时间:齐鲁电子音像出版社

作者:冰的原点

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

<<黑客渗透>>

内容概要

菜鸟起飞,从这里开始!

本笔记将透露:渗透、术语、脚本、内网、溢出各种攻击相关的手段和名词,总结、技巧、细节、亮点,不断变化的攻击思想。

ASP、PHP、JSP等不同类型的脚本漏洞,ACCESS、MYSQL、MSSQL、ORACLE等不同类型的数据库缺陷,国内、国外已知和末知的渗透工具·····

<<黑客渗透>>

作者简介

张开华,网名:冰的原点,2006年9月开始接触网络,并对网络安全产生了浓厚的兴趣而开始自学。 现在湖北武汉求学,专心研究PHP脚本。

虽然学的不是计算机专业,但在大学几年里一直都在关注网络安全。

<<黑客渗透>>

书籍目录

笠 立7/	\ \ =	ᆂᇄᇬᄆ	47.
第一部分	7 八位	前的号	Ħ

- 1.1 基础术语的了解
- 1.2 服务器相关特性
- 1.2.1: windows下的解析特性
- 1.2.2 windows对../的支持
- 1.2.3 windows对空格和.的忽略
- 1.2.4 apache的解析问题
- 1.2.5 不同的系统对大小写的敏感问题
- 1.2.6 实例解析
- 第二部分 小试牛刀--弱口令的软肋
- 2.1 共享入侵 IPC\$
- 2.2 目录浏览
- 2.3 IIS写权限漏洞
- 2.4 暴库
- 2.5 弱口令攻击
- 2.5.1 FTP弱口令
- 2.5.2 基于mssql弱口令的入侵
- 2.5.3 基于mysql弱口令的入侵
- 2.5.4 基于oracle弱口令的入侵
- 2.5.6 tomcat弱口令的入侵
- 2.5.7 第三方管理工具radmin和vnc弱口令入侵

第三部分 犀利的溢出攻击

- 3.1 内存溢出
- 3.2 缓冲区溢出
- 3.2.1 本地溢出
- 3.2.2 远程溢出
- 3.2.3 metasploit工具的使用
- 3.3 exploit杂谈
- 第四部分 流行的web入侵方式
- 4.1 初窥脚本工具
- 4.1.1 扫描工具
- 4.1.2 注入工具
- 4.1.3 数据库类的工具
- 4.1.4 综合检测类工具
- 4.1.5 远控软件
- 4.2 整站系统的利用
- 4.3 各类编辑器的入侵及下载程序在入侵中的作用
- 4.3.1 ewebeditor漏洞串串烧
- 4.3.2 fckeditor漏洞一览
- 4.3.3 不要忘了cuteeditor
- 4.3.4 其它编辑器总结
- 4.3.5 下载工具在渗透中的应用
- 4.4 google大杀器
- 4.4.1 基本语法
- 4.4.2 高级语法

<<黑客渗透>>

- 4.4.3 实战应用
- 4.5 小奏凯歌
- 4.5.1 针对 access数据库的攻击
- 1、上传漏洞
- 2、下载任意文件漏洞
- 3、删除任意文件漏洞
- 4、验证不严漏洞
- 5、直接写一句话木马
- 6、sql注入攻击
- 4.5.2 针对MSSQL数据库的攻击
- 4.5.2.1针对有错误回显的2000数据库的攻击
- 4.5.2.2 针对无错误回显2000数据库的攻击
- 4.5.2.3 针对错误回显2005数据库的攻击
- 4.5.3 针对mysql数据库的攻击
- 4.5.3.1 路径泄露
- 4.5.3.2 本地/远程文件包含漏洞
- 4.5.3.3 文件访问权限验证不严
- 4.5.3.4 上传漏洞
- 4.5.3.5 install文件的风险
- 4.5.3.6 random函数的缺陷
- 4.5.3.7 变量覆盖及变量未初化漏洞
- 4.5.3.8 直接写文件
- 4.5.3.9 直接执行系统命令
- 4.5.3.10 注入攻击
- 4.5.4 针对oracle数据库的攻击
- 4.5.4.1 中间件漏洞一览
- 4.5.4.2 JSP漏洞一览
- 4.5.4.3 注入攻击
- 4.6 剑走偏峰 - 灵巧的旁注

第五部分 忽略的隐患--XSS攻击及其延伸

- 5.1 XSS产生于分析的理论基础
- 5.1.1 XSS的发展概况
- 5.1.2 XSS的存在价值
- 5.1.3 XSS产生的环境及影响
- 5.2 WEB环境中XSS问题的发掘
- 5.2.1 HTML常用代码的属性了解
- 5.2.2 Dom based类型及背景
- 5.2.3 脚本语言代码的使用及变形探讨
- 5.3 如何利用XSS
- 5.3.1对入库型XSS分析
- 5.3.2 对非入库型XSS的分析
- 5.3.3 上传型XSS的分析
- 5.4 总结
- 第六部分 就在身边--社会工程学
- 6.1 间接渗透
- 6.2 直接接触
- 第七部分 巅峰时刻--权限的较量

<<黑客渗透>>

- 7.1 提权概览
- 7.1.1 serv-u提权
- 7.1.2 panywhere提权
- 7.1.3 通过mssql提权
- 7.1.4 通过mysql提权
- 7.1.5 利用radmin提权
- 7.1.6 VNC提权
- 7.1.7 NC反弹
- 7.1.8 JSP、PHP及ASP.NET脚本
- 7.1.9 替换服务
- 7.1.10 autorun.inf提权
- 7.1.11 溢出提权
- 7.1.12 flashxp、leapftp提权
- 7.1.13 G6ftp 提权
- 7.1.14 sinffer提权
- 7.1.15 社工提权
- 7.1.16 提权中注意到的细节
- 7.2 内网渗透
- 7.2.1 信息收集
- 7.2.2 提取系统hash
- 7.2.3 进攻内网
- 7.2.4 细节问题的处理

<<黑客渗透>>

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