

<<Web渗透技术及实战案例解析>>

图书基本信息

书名：<<Web渗透技术及实战案例解析>>

13位ISBN编号：9787121161810

10位ISBN编号：7121161818

出版时间：2012-4

出版时间：电子工业出版社

作者：陈小兵

译者：范渊,孙立伟

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>

## <<Web渗透技术及实战案例解析>>

### 内容概要

本书从Web渗透的专业角度，结合网络安全中的实际案例，图文并茂地再现Web渗透的精彩过程。

本书共分7章，由浅入深地介绍和分析了目前网络流行的Web渗透攻击方法和手段，并结合作者多年的网络安全实践经验给出了相对应的安全防范措施，对一些经典案例还给出了经验总结和技巧，通过阅读本书可以快速掌握目前Web渗透的主流技术。

本书最大的特色就是实用和实战性强，思维灵活。

内容主要包括Web渗透必备技术、Google黑客技术、文件上传渗透技术、SQL注入、高级渗透技术、Oday攻击和Windows提权与安全防范等。

书籍目录

第1章 Web渗透必备技术

1.1 在Windows XP中创建VPN以及使用VPN

1.1.1 创建新的网络连接

1.1.2 选择网络连接类型

1.1.3 选择网络连接

1.1.4 设置VPN显示名称

1.1.5 设置是否自动拨号连接

1.1.6 设置VPN服务器IP地址

1.1.7 设置VPN连接快捷方式

1.1.8 使用VPN连接

1.2 在Windows XP中使用VPN软件

1.2.1 运行VPN客户端

1.2.2 设置VPN

1.2.3 查看本地连接IP地址

1.3 在Windows 2003 Server中建立VPN服务器

1.3.1 查看路由和远程访问

1.3.2 尝试启动路由和远程访问

1.3.3 关闭Windows防火墙

1.3.4 配置并启用路由和远程访问

1.3.5 选择启用的服务

1.3.6 完成服务配置

1.3.7 配置"NAT/基本防火墙"

1.3.8 选择接口

1.3.9 公用接口上启用NAT

1.3.10 启用远程访问和路由

1.3.11 配置日志

1.3.12 授权用户远程访问

1.3.13 VPN连接测试

1.3.14 查看出口IP地址

1.4 LCX端口转发实现内网突破

1.4.1 确定被控制计算机的IP地址

1.4.2 在被控制计算机上执行端口转发命令

1.4.3 在本机上执行监听命令

1.4.4 在本机使用远程终端进行登录

1.4.5 查看本地连接

1.5 域名查询技术

1.5.1 域名小知识

1.5.2 域名在渗透中的作用

1.5.3 使用IP866网站查询域名

1.5.4 使用yougetsignal网站查询域名

1.5.5 使用Acunetix Web VulnerabilityScanner查询子域名

1.5.6 旁注域名查询

1.6 使用GetHashes软件获取Windows系统Hash密码值

1.6.1 Hash基本知识

1.6.2 Hash算法在密码上的应用

## <<Web渗透技术及实战案例解析>>

- 1.6.3 Windows下Hash密码值
- 1.6.4 Windows下NTLM Hash生成原理
- 1.6.5 使用GetHashes获取Windows系统的Hash密码值
- 1.6.6 使用GetHashes获取系统Hash值技巧
- 1.6.7 相关免费资源
- 1.7 使用Saminside获取系统密码
  - 1.7.1 下载和使用Saminside
  - 1.7.2 使用Scheduler导入本地用户的Hash值
  - 1.7.3 查看导入的Hash值
  - 1.7.4 导出系统用户的Hash值
  - 1.7.5 设置Saminside破解方式
  - 1.7.6 执行破解
  - 1.7.7 使用Ophcrack破解用户密码值
- 1.8 使用WinlogonHack获取系统密码
  - 1.8.1 远程终端技术APP和远程终端密码泄露分析
  - 1.8.2 使用WinlogonHack工具软件截取密码原理
  - 1.8.3 使用WinlogonHack获取密码实例
  - 1.8.4 攻击方法探讨
  - 1.8.5 防范方法探讨
- 1.9 使用Ophcrack破解系统Hash密码
  - 1.9.1 通过已有信息再次进行搜索和整理
  - 1.9.2 安装Ophcrack软件
  - 1.9.3 使用Ophcrack软件
  - 1.9.4 下载彩虹表
  - 1.9.5 设置彩虹表
  - 1.9.6 准备破解材料
  - 1.9.7 开始破解
  - 1.9.8 彩虹表破解密码防范策略
- 1.10 MD5加密与解密
  - 1.10.1 有关MD5加解密知识
  - 1.10.2 通过cmd5网站生成MD5密码
  - 1.10.3 通过cmd5网站破解MD5密码
  - 1.10.4 在线MD5破解网站收费破解高难度的MD5密码值
  - 1.10.5 使用字典暴力破解MD5密码值
  - 1.10.6 一次破解多个密码
  - 1.10.7 MD5变异加密方法破解
- 1.11 Serv-U密码破解
  - 1.11.1 获取ServUDAemon.ini文件
  - 1.11.2 查看ServUDAemon.ini文件
  - 1.11.3 破解Serv-U密码
  - 1.11.4 验证Ftp
- 1.12 Access数据库破解实战
  - 1.12.1 Access数据库的基本知识
  - 1.12.2 Access数据库的主要特点
  - 1.12.3 Access数据库的缺点和局限性
  - 1.12.4 Access数据库版本
  - 1.12.5 Access密码实战破解实例

## <<Web渗透技术及实战案例解析>>

### 1.13 巧用Cain破解MySQL数据库密码

#### 1.13.1 MySQL加密方式

#### 1.13.2 MySQL数据库文件结构

#### 1.13.3 获取MySQL数据库用户密码加密字符串

#### 1.13.4 将MySQL用户密码字符串加入到Cain破解列表

#### 1.13.5 使用字典进行破解

#### 1.13.6 破解探讨

### 1.14 SQL Server 2005还原数据库攻略

#### 1.14.1 SQL Server 2005新特性

#### 1.14.2 还原备份数据库

### 1.15 一句话后门利用及操作

#### 1.15.1 执行中国菜刀

#### 1.15.2 添加Shell

#### 1.15.3 连接一句话后门

#### 1.15.4 执行文件操作

#### 1.15.5 有关一句话后门的收集与整理

### 1.16 远程终端的安装与使用

#### 1.16.1 Windows 2000 Server开启远程终端

#### 1.16.2 Windows XP开启远程终端

#### 1.16.3 Windows 2003开启远程终端

#### 1.16.4 一些常见开启远程终端服务的方法

#### 1.16.5 开启远程终端控制案例

#### 1.16.6 命令行开启远程终端

#### 1.16.7 3389实用技巧

## 第2章 Google --爱你又恨你

### 2.1 Google批量注入

#### 2.1.1 使用啊D注入工具搜索SQL注入点

#### 2.1.2 进行SQL注入测试

#### 2.1.3 总结与探讨

### 2.2 Google搜索Web Shell的实际处理思路

#### 2.2.1 通过Google搜索相应的Web Shell关键字

#### 2.2.2 处理搜索结果

#### 2.2.3 破解登录密码

#### 2.2.4 漏洞测试

#### 2.2.5 获取Web Shell

#### 2.2.6 实施控制

#### 2.2.7 总结与探讨

### 2.3 从Aspx的Web Shell到肉鸡

#### 2.3.1 AspxSpy简介

#### 2.3.2 源代码简要分析

#### 2.3.3 动手打造自己的Web Shell

#### 2.3.4 寻找他人的Web Shell

#### 2.3.5 处理获取的Web Shell

#### 2.3.6 总结与探讨

### 2.4 用phpWeb Shell抓肉鸡

#### 2.4.1 使用搜索引擎查找Web Shell

#### 2.4.2 进行相关信息收集

## <<Web渗透技术及实战案例解析>>

- 2.4.3 获取Web Shell与提权
- 2.4.4 总结与探讨
- 2.5 利用JFolder后门渗透某网站
  - 2.5.1 JFolder搜索与测试
  - 2.5.2 Web渗透测试
  - 2.5.3 服务器提权
  - 2.5.4 其他信息获取
  - 2.5.5 总结与探讨
- 2.6 Public权限渗透某asp.net网站
  - 2.6.1 寻找SQL注入点
  - 2.6.2 使用工具进行信息收集和数据猜测
  - 2.6.3 获取SQL注入点
  - 2.6.4 猜解数据库中的表和数据
  - 2.6.5 扫描和获取后台地址
  - 2.6.6 登录测试和验证
  - 2.6.7 寻找、测试和获取Web Shell
  - 2.6.8 尝试提权
  - 2.6.9 登录远程桌面
  - 2.6.10 总结与探讨
- 2.7 对某音乐网站的一次安全检测
  - 2.7.1 获取Web Shell信息
  - 2.7.2 安全检测之信息获取
  - 2.7.3 安全检测之漏洞检测
  - 2.7.4 提权之路
  - 2.7.5 总结与探讨
- 第3章 都是文件上传惹的祸
  - 3.1 利用FCKeditor漏洞渗透某Linux服务器
    - 3.1.1 一个Shell引发的渗透
    - 3.1.2 验证Web Shell
    - 3.1.3 分析Web Shell
    - 3.1.4 上传Web Shell
    - 3.1.5 测试上传的Web Shell
    - 3.1.6 对Web Shell所在服务器进行分析与信息收集
    - 3.1.7 服务器提权
    - 3.1.8 总结与探讨
  - 3.2 渗透某培训网站
    - 3.2.1 使用Jsky进行漏洞扫描
- .....

章节摘录

版权页：插图：

## <<Web渗透技术及实战案例解析>>

### 编辑推荐

《Web渗透技术及实战案例解析》由浅入深依照Web攻防的一些技术特点安排内容，每一小节都是一个具体Web攻防技术的典型应用，同时结合案例给予讲解，并给出一些经典的总结。实用性强可供对网络安全感兴趣的读者使用，同时也适合作为计算机应用专业高年级本科生和研究生的网络安全课程实践参考资料。

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>