

<<黑客工具全程揭秘>>

图书基本信息

书名：<<黑客工具全程揭秘>>

13位ISBN编号：9787113128852

10位ISBN编号：7113128858

出版时间：2012-1

出版时间：中国铁道

作者：张齐

页数：256

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>

## <<黑客工具全程揭秘>>

### 内容概要

本书分10章围绕当前黑客主流工具展开，囊括最新的攻击手段和防护技巧，涵盖了从系统底层到网络应用层的多方面知识。

本书主要针对掌握基础计算机知识，对网络安全兴趣浓厚的朋友；对黑客技术感兴趣，但未经过系统学习的读者；网络攻击与防护初级学者以及网络管理者。

# <<黑客工具全程揭秘>>

## 书籍目录

### chapter 01 了解黑客

#### 1.1 黑客简介

1.1.1 是黑客不是骇客

1.1.2 黑客宗旨：网络资源共享

1.1.3 黑客常用哪几招

1.1.4 黑客工具亮一亮

#### 1.2 黑客命令

1.2.1 ping命令

1.2.2 net命令

1.2.3 telnet命令

1.2.4 rp命令

1.2.5 arp命令

1.2.6 netstat命令

1.2.7 tracert命令

1.2.8 ipconfig命令

1.2.9 route命令

1.2.10 netsh命令

### chapter 02 计算机安全知识

#### 2.1 无处不在的漏洞

2.1.1 什么是漏洞

2.1.2 系统漏洞概述

2.1.3 常见漏洞解析

#### 2.2 黑客通道：端口

2.2.1 端口的概念

2.2.2 查看端口

2.2.3 关闭/限制端口

2.2.4 重要端口解析

#### 2.3 权限之争：账户

2.3.1 了解计算机账户

2.3.2 管理员账户

2.3.3 账户的建立方式

#### 2.4 无处不在的进程

2.4.1 什么是进程

2.4.2 进程与病毒

2.4.3 进程操作

### chapter 03 扫描工具

#### 3.1 端口扫描

3.1.1 端口扫描工具原理

3.1.2 常用扫描工具

3.1.3 网络端口扫描命令

#### 3.2 x-scan扫描器

3.2.1 x-scan简介

3.2.2 x-scan配置

3.2.3 x-scan扫描指南

3.2.4 x-scan扩展工具

## <<黑客工具全程揭秘>>

- 3.2.5x-scan常见问题
- 3.3superscan扫描器
  - 3.3.1superscan简介
  - 3.3.2superscan附属工具
- 3.4s扫描器
  - 3.4.1s扫描器简介
  - 3.4.2s扫描器扫描指南
- 3.5nmap扫描器
  - 3.5.1nmap扫描器简介
  - 3.5.2nmap扫描器配置
- 3.6特殊扫描器
  - 3.6.1sss扫描器
  - 3.6.2sql扫描器
  - 3.6.3流光溯雪
  - 3.6.4溯雪
- chapter 04 注入工具
  - 4.1啊d注入工具
    - 4.1.1功能介绍
    - 4.1.2注入实战
  - 4.2暴库
  - 4.3nbsi注入工具
    - 4.3.1 nbsi的概述
    - 4.3.2nbsi入侵
  - 4.4 domain注入工具
    - 4.4.1domain功能简介
    - 4.4.2注入攻击
    - 4.4.3旁注思路
    - 4.4.4asp木马
    - 4.4.5防范asp木马
  - 4.5 wis注入工具
    - 4.5.1利用wis注入工具寻找注入点
    - 4.5.2利用sql注入破解管理员账号
  - 4.6如何防止注入攻击
  - 4.7对于非asp网站注入研究
- chapter 05 嗅探工具
  - 5.1影音嗅探
  - 5.2iris嗅探器
    - 5.2.1了解iris嗅探器
    - 5.2.2用iris嗅探数据
  - 5.3聚生网管
    - 5.3.1聚生网管配置
    - 5.3.2聚生网管应用
  - 5.4密码监听器
    - 5.5cookie嗅探
      - 5.5.1利用cookie给论坛灌水
      - 5.5.2利用cookie当版主
      - 5.5.3管理cookie

## <<黑客工具全程揭秘>>

### 5.6arp嗅探

5.6.1winarpattacker介绍

5.6.2winarpattacker功能

### 5.7防止arp攻击

5.7.1antiarp snieer

5.7.2奇虎arp防火墙

## chapter 06 qq工具

### 6.1qq辅助工具

6.1.1强制qq聊天

6.1.2liteimì调控qq

6.1.3整合qq聊天

6.1.4巧妙搜索qq用户

### 6.2qq安全

6.2.1qq木马

6.2.2qq安全指南

6.2.3本地qq攻防

6.2.4阿拉qq大盗

### 6.3钓鱼攻击

6.3.1网络钓鱼简介

6.3.2netcrafttoolbar避免成为盘中餐

6.3.3其他钓鱼方式

6.3.4防止网络钓鱼准则

## chapter 07 木马工具

### 7.1木马9a6c的概念

7.1.1木马的构成

7.1.2木马攻击流程

7.1.3常见木马分类

### 7.2木马伪装方式

7.2.1加壳与脱壳

7.2.2文件合并种植木马

7.2.3自定义文件夹种植木马

7.2.4网页种植木马

7.2.5chm电子书种植木马

7.2.6免杀木马

### 7.3木马的清除与防范

7.3.1360安全卫士清除木马

7.3.2木马克星iparmor

7.3.3thecleaner清除木马

7.3.4手动查杀系统中的隐藏木马

## chapter 08 加密解密工具

### 8.1加密工具

8.1.1文件加密

8.1.2图片加密

8.1.3网页加密

8.1.4密码再加密

8.1.5无线网络加密

8.1.6加密新思路

<<黑客工具全程揭秘>>

8.1.7用u盘加密电脑

8.2解密工具

8.2.1破解系统密码

8.2.2破解压缩密码

8.2.3破解office密码

8.2.4网络密码破解

8.2.5密码保护箱

chapter 09 远程控制工具

9.1冰河

9.1.1认识冰河

9.1.2应用冰河

9.1.3配置冰河

9.1.4清除冰河

9.2灰鸽子

9.2.1认识灰鸽子

9.2.2配置灰鸽子

9.2.3使用灰鸽子

9.2.4清除灰鸽子

9.3radmin

9.3.1radmin简介

9.3.2radmin配置

9.3.3连接radmin

chapter 10 安全工具

10.1杀毒软件

10.1.1瑞星杀毒软件

10.1.2esetnod32

10.2防火墙

10.2.1系统防火墙

10.2.2天网防火墙

写在最后

附录a 注册表操作攻略

系统应用

网络应用

系统优化

系统美化

硬件优化

软件设置

添加右键选项

改变目录

更改图标

更改提示信息

禁止菜单

## 章节摘录

版权页：插图：加强对用户输入的验证。

总体来说，防治SQL注入式攻击可以采用两种方法：一是加强对用户输入内容的检查与‘验证’；二是强迫使用参数化语句来传递用户输入的内容。

在SQLServer数据库中，有比较多的用户输入内容验证工具，可以帮助管理员来对付SQL注入式攻击。

测试字符串变量的内容，只接受所需的值。

拒绝包含二进制数据、转义序列和注释字符的输入内容。

这有助于防止脚本注入，防止某些缓冲区溢出攻击。

测试用户输入内容的大小和数据类型，强制执行适当的限制与转换。

这即有助于防止有意造成的缓冲区溢出，对于防治注入式攻击有比较明显的效果。

可以使用存储过程来验证用户的输入。

利用存储过程可以实现对用户输入变量的过滤，拒绝一些特殊的符号。

以上那个恶意代码中，只要存储过程把那个分号过滤掉，那么这个恶意代码也就没有用武之地了。

在执行SQL语句之前，可以通过数据库的存储过程，来拒绝接纳一些特殊的符号。

在不影响数据库应用的前提下，应该让数据库拒绝包含以下字符的输入。

分号分隔符，它是SQL注入式攻击的主要帮凶，如注释分隔符。

注释只有在数据设计的时候用的到。

一般用户的查询语句中没有必要注释的内容，可以直接把它拒绝掉，通常情况下这么做不会发生意外损失。

把以上这些特殊符号拒绝掉，那么即使在SQL语句中嵌入了恶意代码，他们也将毫无作为。

始终通过测试类型、长度、格式和范围来验证用户输入，过滤用户输入的内容。

这是防止SQL注入式攻击的常见并且行之有效的措施。

多使用SQLServer数据库自带的安全参数。

为了减少注入式攻击对于SQLServer数据库的不良影响，在SQLServer数据库专门设计了相对安全的SQL参数。

在数据库设计过程中，工程师要尽量采用这些参数来杜绝恶意的SQL注入式攻击。

必要的情况下使用专业的漏洞扫描工具来寻找可能被攻击的点。

使用专业的漏洞扫描工具，可以帮助管理员来寻找可能被SQL注入式攻击的点。

不过漏洞扫描工具只能发现攻击点，而不能主动起到防御SQL注入攻击的作用。

当然这个工具也经常攻击者拿来使用，如攻击者可以利用这个工具自动搜索攻击目标并实施攻击。

为此在必要的情况下，应当投资于一些专业的漏洞扫描工具。

一个完善的漏洞扫描程序不同于网络扫描程序，它专门查找数据库中的SQL注入式漏洞。

最新的漏洞扫描程序可以查找最新发现的漏洞。

所以凭借专业的工具，可以帮助管理员发现SQL注入式漏洞，并提醒管理员采取积极的措施来预防SQL注入式攻击。

如果攻击者能够发现的SQL注入式漏洞数据库管理员都发现了并采取了积极的措施堵住漏洞，那么攻击者也就无从下手了。

## <<黑客工具全程揭秘>>

### 编辑推荐

《黑客工具全程揭秘》：紧贴行业热点、精选热门工具、攻防融合一体、为读者呈现最新的安全知识、实际操作为先学习不再枯燥、知道攻击原理还懂怎么防护。

我们的目的不是教你如何攻击，而是告诉你怎样防护，对于网络世界来说，安全永远比攻击更重要。

《黑客工具全程揭秘》内容只是黑客世界中的一部分，但却可以帮助你打开信息安全领域的大门。

《黑客工具全程揭秘》是了解黑客，学习安全知识的一把全钥匙！

结合丰富案例，上手更加简单穿插生动漫画，降低学习难度一书籍在手，黑客工具全懂此书秉承黑客理念，贯穿黑客入侵全过程，旨在让广大读者了解黑客是如何入侵，攻击的，并结出相应的防护方法。

<<黑客工具全程揭秘>>

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>