

# 《Linux网络安全技术与实现》

## 图书基本信息

书名：《Linux网络安全技术与实现》

13位ISBN编号：9787302278863

10位ISBN编号：7302278865

出版时间：2012-3

出版社：清华大学出版社

作者：陈勇勋

页数：494

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《Linux网络安全技术与实现》

## 内容概要

《Linux网络安全技术与实现(第2版)》是一本将理论与实践完美结合的书。从网络的基本概念开始，采用由浅入深的方式，逐步引导读者进入网络安全的世界，让读者从无到有地快速理解，以帮助愿意迈入网络安全领域的IT技术人员，完整、正确地构建企业网络的安全屏障。

# 《Linux网络安全技术与实现》

## 作者简介

现任 精诚资讯知识产品事业部资深讲师兼产品经理 专长

Linux系统管理、防火墙及VPN规划、数字证书管理、OpenLDAP规划、Linux服务器及企业网络规划、Linux与Windows系统整合、企业网络病毒防治、PHP&MySQLN站开发及构建、带宽合并及管理、虚拟化技术

认证 RHCE、RHCX、TigerTeam Class C+P2P、RHCVA

## 书籍目录

### 第1章 防火墙的基本概念

#### 1.1 TCP/IP的基本概念

##### 1.1.1 应用层

##### 1.1.2 传输层

##### 1.1.3 网络层

##### 1.1.4 链路层

#### 1.2 数据包传输

#### 1.3 TCP、UDP及Socket的关系

#### 1.4 何谓防火墙

#### 1.5 防火墙的判断依据

##### 1.5.1 各层数据包包头内的信息

##### 1.5.2 数据包所承载的数据内容

##### 1.5.3 连接状态

#### 1.6 防火墙的分类

##### 1.6.1 数据包过滤防火墙

##### 1.6.2 应用层防火墙

#### 1.7 常见的防火墙结构

##### 1.7.1 单机防火墙

##### 1.7.2 网关式防火墙

##### 1.7.3 透明防火墙

#### 1.8 小结

### 第2章 Netfilter/iptables

#### 2.1 何谓内核

#### 2.2 何谓Netfilter

#### 2.3 Netfilter与Linux的关系

#### 2.4 Netfilter工作的位置

#### 2.5 Netfilter的命令结构

#### 2.6 Netfilter的filter机制

#### 2.7 规则的匹配方式

#### 2.8 Netfilter与iptables的关系

#### 2.9 iptables工具的使用方法

##### 2.9.1 iptables命令参数

##### 2.9.2 iptables规则语法

##### 2.9.3 学以致用：iptables的规则语法

#### 2.10 使用iptables机制来构建简单的单机防火墙

##### 2.10.1 如何测试防火墙规则正确与否

##### 2.10.2 解决无法在防火墙主机上对外建立连接的问题

##### 2.10.3 管理防火墙规则数据库的办法

#### 2.11 使用filter机制来构建网关式防火墙

#### 2.12 Netfilter的NAT机制

##### 2.12.1 IP网段的划分

##### 2.12.2 私有IP

##### 2.12.3 NAT

##### 2.12.4 数据包传输方向与SNAT及DNAT的关系

##### 2.12.5 NAT的分类

##### 2.12.6 NAT并非无所不能

#### 2.13 Netfilter的Mangle机制

2.14 Netfilter的raw机制

2.15 小结

第3章 Netfilter的匹配方式及处理方法

3.1 匹配方式

3.1.1 内置的匹配方式

3.1.2 从模块扩展而来的匹配方式

3.2 处理方法

3.2.1 内置的处理方法

3.2.2 由模块扩展的处理方法

3.3 小结

第4章 Netfilter/Iptables的高级技巧

4.1 防火墙性能的最优化

4.1.1 调整防火墙规则顺序

4.1.2 巧妙使用multiport及iprange模块

4.1.3 巧妙使用用户定义的链

4.2 Netfilter连接处理能力与内存消耗

4.2.1 计算最大连接数

4.2.2 调整连接跟踪数

4.2.3 连接跟踪数量与内存消耗

4.3 使用raw表

4.4 简单及复杂通信协议的处理

4.4.1 简单通信协议

4.4.2 复杂通信协议

4.4.3 ICMP数据包的处理原则

4.4.4 在DMZ上使用NAT将面临的问题及解决方案

4.4.5 常见的网络攻击手段及防御方法

4.5 小结

第5章 代理服务器的应用

5.1 何谓代理服务器

5.2 代理服务器支持的通信协议

5.3 代理服务器的分类

5.3.1 何谓缓存代理

5.3.2 何谓反向代理

5.4 代理服务器的硬件要求

5.5 安装Squid代理

5.6 使用Squid构建缓存代理

5.6.1 缓存代理的基本配置

5.6.2 缓存代理客户端的配置

5.6.3 缓存代理的高级配置

5.6.4 缓存代理连接访问控制

5.6.5 缓存对象的管理

5.6.6 Squid代理的工作日志

5.6.7 Squid代理的名称解析

5.7 透明代理

5.7.1 透明代理的工作原理

5.7.2 透明代理的配置

5.8 反向代理

5.8.1 Web服务器的分类

5.8.2 构建反向代理

## 5.9 小结

## 第6章 使用Netfilter/Iptables保护企业网络

### 6.1 防火墙结构的选择

### 6.2 防火墙本机的安全

#### 6.2.1 网络攻击

#### 6.2.2 系统入侵

#### 6.2.3 入站/出站的考虑事项

#### 6.2.4 远程管理的安全考虑事项

### 6.3 防火墙的规则定义

#### 6.3.1 企业内部与因特网

#### 6.3.2 DMZ与因特网

#### 6.3.3 企业内部与DMZ

### 6.4 入侵与防御的其他注意事项

#### 6.4.1 更新系统软件

#### 6.4.2 Syn Flooding攻击防御

#### 6.4.3 IP欺骗防御

## 6.5 小结

## 第7章 Linux内核编译

### 7.1 为何需要重新编译内核

### 7.2 内核编译

#### 7.2.1 安装软件开发环境

#### 7.2.2 获取内核源代码

#### 7.2.3 整合源代码

#### 7.2.4 设置编译完成后的内核版本号

#### 7.2.5 清理内核源代码以外的临时文件

#### 7.2.6 设置内核编译参数

#### 7.2.7 执行编译操作

#### 7.2.8 安装模块及结构中心

#### 7.2.9 修改开机管理程序

### 7.3 如何安装内核补丁

#### 7.3.1 下载补丁文件及内核源代码

#### 7.3.2 准备内核及补丁的源代码

#### 7.3.3 运行内核补丁

#### 7.3.4 设置内核编译参数

#### 7.3.5 内核编译完毕后的检查

## 7.4 小结

## 第8章 应用层防火墙

### 8.1 如何为iptables安装补丁

### 8.2 Layer7模块识别应用层协议的原理

### 8.3 安装Layer7模块的模式

### 8.4 如何使用Layer7模块

### 8.5 Layer7模块使用示例说明

### 8.6 结合使用包过滤器与Layer7模块

## 8.7 小结

## 第9章 透明式防火墙

### 9.1 何谓桥接模式

### 9.2 何谓透明式防火墙

### 9.3 构建透明式防火墙

#### 9.3.1 使用Linux构建网桥

9.3.2 Netfilter在Layer3及Layer2的工作逻辑

9.3.3 另一种透明式防火墙

9.3.4 配置代理ARP

9.4 小结

第 10 章 基于策略的路由及多路带宽合并

10.1 何谓基于策略的路由

10.2 了解Linux的路由机制

10.3 路由策略数据库与路由表的管理

10.3.1 管理策略数据库

10.3.2 管理路由表

10.4 带宽合并

10.4.1 何谓带宽合并

10.4.2 企业内的带宽合并

10.5 小结

第 11 章 Linux的带宽管理

11.1 队列

11.1.1 不可分类的队列算法

11.1.2 可分类的队列算法

11.2 Linux带宽管理

11.3 过滤器

11.3.1 FW过滤器

11.3.2 U32过滤器

11.4 带宽管理部署示例

11.4.1 带宽划分

11.4.2 设置队列算法

11.4.3 设置队列规则

11.4.4 设置过滤器

11.4.5 测试

11.5 带宽借用

11.6 类别中的队列

11.7 Linux带宽管理的限制

11.8 网桥模式中的带宽管理

11.9 多接口的带宽管理

11.9.1 为内核及iptables安装补丁

11.9.2 多接口带宽管理

11.10 实际案例

11.11 小结

第 12 章 流量统计

12.1 安装及测试SNMP服务器

12.1.1 安装SNMP服务器

12.1.2 测试SNMP服务器

12.2 安装及设置MRTG

12.2.1 安装MRTG

12.2.2 设置MRTG

12.2.3 使用cfgmaker工具编写MRTG针对网卡的配置文件

12.3 另一种网络流量监测方式

12.3.1 结合使用Netfilter/Iptables和MRTG来监测网络流量

12.3.2 手动编写MRTG的配置文件

12.4 外部程序及MRTG配置文件的示例

## 12.5 小结

## 第 13 章 弱点扫描、入侵检测及主动防御系统

### 13.1 何谓弱点扫描

#### 13.1.1 OpenVAS弱点扫描工具

#### 13.1.2 OpenVAS弱点扫描工具的工作架构

#### 13.1.3 下载及安装OpenVAS弱点扫描工具

#### 13.1.4 进行弱点扫描

### 13.2 入侵检测系统

#### 13.2.1 网络设备的限制

#### 13.2.2 入侵检测系统的分类

#### 13.2.3 入侵检测系统的部署

#### 13.2.4 Snort入侵检测系统介绍

#### 13.2.5 下载及安装Snort入侵检测系统

#### 13.2.6 下载及安装Snort的规则数据库

#### 13.2.7 配置Snort

#### 13.2.8 Snort的启停

#### 13.2.9 Snort的警告

### 13.3 主动防御系统

#### 13.3.1 下载Guardian

#### 13.3.2 安装Guardian

#### 13.3.3 设置Guardian

#### 13.3.4 Guardian的启停

## 13.4 小结

## 第 14 章 VPN基础篇

### 14.1 何谓VPN

#### 14.1.1 VPN的原理

#### 14.1.2 常见的VPN架构

#### 14.1.3 VPN的安全问题

#### 14.1.4 VPN机制的优缺点

### 14.2 数据加解密

#### 14.2.1 何谓“明文”

#### 14.2.2 何谓“密文”

### 14.3 数据加密类型

#### 14.3.1 对称加密

#### 14.3.2 非对称加密

### 14.4 哈希算法

#### 14.4.1 常见的哈希算法

#### 14.4.2 哈希算法的特性

### 14.5 基于IPSec的VPN

#### 14.5.1 IPSec的工作模式

#### 14.5.2 IPSec的组成要素

#### 14.5.3 AH及ESP协议运行时需要设置的参数

#### 14.5.4 安装IPSec参数的管理工具

#### 14.5.5 配置传输模式IPSec VPN

### 14.6 Linux中的IPSec架构

#### 14.6.1 IPSec机制的SPD

#### 14.6.2 IPSec机制的SAD

## 14.7 小结

## 第 15 章 VPN实战篇



- 15.1 IKE
- 15.2 Preshared Keys验证模式下的传输模式VPN
  - 15.2.1 数据库服务器的设置
  - 15.2.2 客户端主机的设置
  - 15.2.3 启动VPN
- 15.3 Preshared Keys验证模式下的隧道模式VPN
  - 15.3.1 VPN 服务器(A)主机上的设置
  - 15.3.2 VPN 服务器(B)主机上的设置
- 15.4 何谓数字证书
  - 15.4.1 数字证书的必要性
  - 15.4.2 证书管理中心
  - 15.4.3 将Linux系统作为企业的CA
- 15.5 数字证书验证模式下的传输模式VPN
  - 15.5.1 证书的生成及保存
  - 15.5.2 客户端VPN主机的设置
- 15.6 数字证书验证模式下的隧道模式VPN
  - 15.6.1 证书的生成及保存
  - 15.6.2 设置VPN 服务器(A)
  - 15.6.3 设置VPN 服务器(B)
  - 15.6.4 启动IPSec
- 15.7 小结
- 第 16 章 VPN : L2TP Over IPSec
  - 16.1 何谓PPP
  - 16.2 何谓L2TP协议
    - 16.2.1 L2TP协议的原理
    - 16.2.2 L2TP协议的安全问题
    - 16.2.3 L2TP协议安全问题的解决方案
    - 16.2.4 Client to Site的L2TP VPN结构探讨
    - 16.2.5 L2TP 客户端及服务器之间网段的选择
    - 16.2.6 Proxy ARP的工作原理
  - 16.3 构建L2TP VPN
    - 16.3.1 配置L2TP服务器
    - 16.3.2 配置PPP服务器
    - 16.3.3 建立VPN的拨号帐户
    - 16.3.4 证书的生成及保存
    - 16.3.5 配置安全策略
    - 16.3.6 IKE配置文件
    - 16.3.7 启动L2TP服务器
  - 16.4 配置L2TP客户端
    - 16.4.1 生成L2TP客户端证书
    - 16.4.2 将证书导入Windows XP/7系统前的准备工作
    - 16.4.3 设置Windows XP系统上的L2TP客户端
    - 16.4.4 设置Windows 7系统中的L2TP客户端
  - 16.5 IPSec连接穿透NAT的问题
  - 16.6 小结

## 章节摘录

版权页：插图：3.RELATED 另一个重要的状态是RELATED，这个状态在“高级防火墙规则”中也是很重要的，但现阶段不介绍RELATED状态的应用，在第3.1.2一节的第8部分将会有完整且详细的说明。不过，我们还是可以先大略了解什么是RELATED状态。你应该有在Windows平台上使用tracert这个命令的经验吧！图2.31即为tracert命令执行的结果，而这个工具的目的就是让我们去检测两台主机之间，总共间隔了多少个路由器。但你是否曾经想过这个工具的工作原理？其实tracert工具的工作原理相当简单，首先我们得从IP包头中的TTL值谈起，这个TTL值是指数据包在网络上所能存活的时间，在早期是以秒为单位，不过，现在则改为“所能跨越的路由器数量”。下面以图2—32为例来看看tracert工具是如何查询图中最右边与最左边的主机，且总共间隔了多少个路由器？首先tracert工具会发送第一个数据包，这个数据包的目的端IP就是最左边主机的IP，并且可以将这个数据包的TTL值设定为1。接着，这个数据包就被送到第一个路由器1，而第一个路由器在收到这个数据包之后，即将数据包内的TTL值减1，因此，这个数据包的TTL值变为0，这个值代表数据包生命周期已尽，所以第一个路由器即会丢弃这个数据包，并且回送一个ICMP Type 11 (Time to live exceeded) 的数据包给包的发送端主机，告知“你发送的数据包因生命周期已尽，故已遭到丢弃”，如此tracert工具就可从这个ICMP数据包得知第一个路由器的IP地址。tracert接着会送出第二个数据包，不过，这个数据包的TTL值会特意设置为2，接着，第二个数据包会被送到第一个路由器1，第一个路由器收到这个数据包之后，会将其TTL值减1，这是数据包内的TTL值将会变为1，因为TTL值不为0，故其生命周期未尽，因此第一个路由器会将这个数据包转发给第二个路由器2。不过，当第二个路由器把数据包内的TTL减1之后，这个数据包内的TTL值即为0，代表这个数据包的生命周期已尽，因此第二个路由器即会丢弃这个数据包，并且回送一个ICMP Type 11 (Time to live exceeded) 的数据包给发送端主机，告知“你所发送的数据包因生命周期已尽，故已遭到丢弃”。如此一来，tracert工具就可从这个ICMP数据包得知第二个路由器的IP地址。

## 精彩短评

- 1、才到手，粗看了下，感觉很不错。支持原创。
- 2、感觉讲的很细。收获挺大
- 3、是正版的，正学这本书
- 4、还不错,讲得挺好的
- 5、书的内容不错，快递也很快，但是书的封皮太差了，很脏，很旧，有磨损
- 6、轻松掌握netfilter的优秀教材
- 7、当当卖书还是比较靠谱的，
- 8、书不错,书中将linux防火的各方面讲解的很深刻,脚本很不错,具有很好的实践价值!
- 9、讲解清晰，还不错，挺实用的
- 10、没看明白一些安全问题如何实现的，如何防护，只是理论的说明多些。。
- 11、比较详细，通俗
- 12、我去年买了个表
- 13、学习至上
- 14、很实用的教材，有一定linux和网络安全基础阅读掌握很快
- 15、不错，很实用，很适合搭建可用的网络环境。初学者必备啊。
- 16、内容通俗易懂，快递太慢了，前后发货5天
- 17、很实用的一本书，通俗易懂
- 18、深入浅出，详细地介绍网络原理和设置思路。
- 19、技术的书，我不懂
- 20、这本书写的不错，比较全面
- 21、最基本的概念，对于起步阶段还是有点用，可惜主要都只是介绍netfilter/iptables的操作。
- 22、强力推荐！浅显易懂，LINUX网络学习强力推荐！不过需要注意的是，不分专业名词台湾的叫法和内地有区别。几个同事看了我的书后，都去买了一本。
- 23、好,不错
- 24、这本书对我帮助很大，刚好和我们现在学习的课程一样。
- 25、想看安全的可以看下
- 26、iptables规则使用说明书~
- 27、推荐学习linux安全的的朋友买一本
- 28、不错的netfilter书籍，推荐后端/运维看看
- 29、好书，但是给我发的书页面都有点发黄了
- 30、让我完全掌握了netfilter/iptables
- 31、很好的一本书，基础概念清晰易懂，初学者必备。
- 32、值得学习
- 33、学习LINUX不可缺少的
- 34、书里的内容和作者之前的一本书一模一样的，只不过换了名字，但是很值得一读，重点是iptables的知识。
- 35、可以读一下，但书内很多错误，特别是插图。
- 36、不错的书，讲的内容很有体系，特别适合初学者使用。
- 37、看过第一版，写得很好，感觉这一版与第一版的风格不太一样，字也小了很多。
- 38、安全方面开了很多眼界
- 39、iptables, 路由, vpn
- 40、书很不错，对网络的安全性如何部署还是有一定借鉴的
- 41、当当快递太快了，头天下午提交订单，第二天上午就到了
- 42、这书还没怎么看过。。。

## 精彩书评

- 1、最近在做宽带路由器测试的培训，从图书馆借来这本书看。1-4章看了2礼拜，简直就是iptables的深度教学，而且背景知识介绍的很好，适合有基本网络基础知识的IT从业者学习。目前市面上的家用宽带路由，基本都是用嵌入式linux+iptables组的。所以看完此书以后，对宽带路由测试的理解更加深入，对工作帮助不少~~~BTW:边读边用Xmind做了思维导图的读书笔记，传到新浪共享资料去了，有兴趣的可以去看。
- 2、刚看完这本书，总体感觉很不错。采用通俗易懂的实例，由简入繁一步一步地介绍网络安全的相关知识和技术，基本囊括了网络安全相关的话题，书中提供的例子以及工具都很实用，很适合刚开始接触Linux网络安全的初学者，总体来说很不错！

## 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:[www.tushu000.com](http://www.tushu000.com)