

<<开放源码邮件系统安全>>

图书基本信息

书名：<<开放源码邮件系统安全>>

13位ISBN编号：9787115100818

10位ISBN编号：7115100810

出版时间：2002-4

出版时间：人民邮电出版社

作者：RichardBlum

页数：324

字数：512

译者：杜鹃

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>

<<开放源码邮件系统安全>>

内容概要

本书对开放源码电子邮件系统及其安全做了全面而详细深入的介绍。

全书分为三个部分17章。

第一部分包括1到6章，介绍了电子邮件系统的基础知识。

第二部分是7到13章，选取了目前最为流行的3种开放源码邮件软件sendmail、qmail和Postfix，有针对性地介绍了怎样使用它们建立安全的邮件环境，另外着重介绍了防止开放式转发和阻挡垃圾邮件的方法。

第三部分是14到17章，介绍了邮件服务安全方面的高级知识，包括防火墙、SASL、POP3和IMAP服务器安全等技术。

本书内容安排循序渐进，实例丰富，无论是对专业的电子邮件管理员还是普通的电子邮件技术学习者均能有所帮助。

<<开放源码邮件系统安全>>

书籍目录

第一部分 电子邮件原理

第1章 电子邮件基础知识

1.1 UNIX电子邮件系统

1.1.1 UNIX邮件分发代理(MDA)

1.1.2 UNIX邮件传输代理(MTA)

1.1.3 UNIX邮件用户代理(MUA)

1.2 电子邮件协议

1.2.1 邮件传输代理协议(MTA Protocols)

1.2.2 邮件用户代理协议(MUA Protocols)

1.3 邮件安全

1.3.1 避免开放式转发

1.3.2 防止垃圾邮件

1.3.3 防范病毒

1.4 小结

第2章 SMTP协议

2.1 SMTP描述

2.1.1 基本的SMTP客户端命令

2.1.2 服务器应答

2.2 扩展SMTP

2.2.1 ETRN命令

2.2.2 AUTH命令

2.3 邮件格式

2.3.1 标准RFC822邮件头区域

2.3.2 在SMTP邮件事务处理中使用RFC822格式

2.4 小结

第3章 POP3协议

3.1 邮局协议概述

3.2 POP3认证方式

3.2.1 USER/PASS 命令

3.2.2 APOP命令

3.2.3 AUTH命令

3.3 POP3客户端命令

3.3.1 STAT命令

3.3.2 LIST命令

3.3.3 RETR命令

3.3.4 DELE命令

3.3.5 UIDL命令

3.3.6 TOP命令

3.3.7 NOOP命令

3.3.8 RSET命令

3.3.9 QUIT命令

3.4 开放源码POP3协议的实现

3.4.1 开放源码POP3协议客户端

3.4.2 开放源码POP3协议服务器

3.5 小结

<<开放源码邮件系统安全>>

第4章 IMAP协议

4.1 交互邮件访问协议(IMAP)概述

4.2 IMAP认证方法

4.2.1 LOGIN命令

4.2.2 AUTHENTICATE命令

4.3 IMAP客户端协议

4.3.1 SELECT命令

4.3.2 EXAMINE命令

4.3.3 CREATE命令

4.3.4 DELETE命令

4.3.5 RENAME命令

4.3.6 SUBSCRIBE命令

4.3.7 UNSUBSCRIBE命令

4.3.8 LIST命令

4.3.9 LSUB命令

4.3.10 STATUS命令

4.3.11 APPEND命令

4.3.12 CHECK命令

4.3.13 CLOSE命令

4.3.14 EXPUNGE命令

4.3.15 SEARCH命令

4.3.16 FETCH命令

4.3.17 STORE命令

4.3.18 COPY命令

4.3.19 UID命令

4.3.20 CAPABILITY命令

4.3.21 NOOP命令

4.3.22 LOGOUT命令

4.4 开放源码IMAP协议的实现

4.4.1 开放源码IMAP协议服务器

4.4.2 开放源码IMAP协议客户端

4.5 小结

第5章 MIME协议

5.1 Unencode程序

5.1.1 二进制数据编码

5.1.2 二进制数据解码

5.2 MIME和二进制数据

5.2.1 MIME头字段

5.3 S/MIME

5.3.1 S/MIME Multipart子类型

5.3.2 S/MIME application子类型

5.4 开放源码MIME软件包

5.4.1 Metamail工具

5.4.2 Reformime工具

5.5 MIME中使用PGP

5.5.1 安装PGP

5.5.2 使用PGP加密邮件

<<开放源码邮件系统安全>>

5.5.3 使用PGP解密邮件

5.6 小结

第6章 读取邮件头

6.1 解码伪造的邮件头

6.1.1 To:字段

6.1.2 Received:字段

6.1.3 Message-ID:字段

6.2 使用DNS程序追查邮件主机

6.2.1 Whois程序

6.2.2 Nslookup程序

6.2.3 Dig程序

6.3 使用外部的防止垃圾邮件的服务

6.3.1 SpamCop网站

6.3.2 Sam Spade网站

6.4 小结

第二部分 服务器安全

第7章 保护UNIX服务器安全

7.1 监视日志文件

7.1.1 Syslogd进程

7.1.2 Syslogd配置文件

7.1.3 监视攻击

7.2 防范网络攻击

7.2.1 使用Inetd程序

7.2.2 Inetd配置文件

7.2.3 关闭不需要的服务

7.3 拒绝通过网络访问服务器

7.3.1 安装Ipchains

7.3.2 使用Ipchains

7.3.3 保存Ipchains过滤器

7.3.4 Ipchains示例

7.3.5 Bastille工程

7.4 入侵检测

7.4.1 下载并安装Tripwire

7.4.2 配置Tripwire

7.4.3 运行Tripwire

7.5 小结

第8章 sendmail邮件软件

8.1 什么是sendmail

8.2 配置sendmail

8.2.1 D行

8.2.2 C行

8.2.3 F行

8.2.4 K行

8.2.5 H行

8.2.6 M行

8.2.7 P行

8.2.8 O行

<<开放源码邮件系统安全>>

- 8.2.9 规则集行
- 8.3 使用m4预处理器
- 8.4 sendmail命令行
- 8.5 安装sendmail
 - 8.5.1 获取并编译源码
 - 8.5.2 创建和安装配置文件
 - 8.5.3 启动并测试sendmail
- 8.6 保障sendmail安全
 - 8.6.1 文件权限
 - 8.6.2 sendmail用户
 - 8.6.3 受信应用
- 8.7 小结
- 第9章 qmail邮件软件
 - 9.1 什么是qmail
 - 9.2 控制文件
 - 9.2.1 控制文件结构
 - 9.2.2 qmail控制文件
 - 9.3 下载并编译qmail源码
 - 9.3.1 编译前的项目检查
 - 9.3.2 编译qmail
 - 9.4 配置qmail
 - 9.4.1 创建基本的qmail控制文件
 - 9.4.2 创建必要的qmail别名
 - 9.4.3 选择本地邮件发送方式
 - 9.5 使用qmail sendmail包装程序
 - 9.6 接收SMTP邮件
 - 9.7 qmail和安全
 - 9.8 小结
- 第10章 Postfix邮件软件
 - 10.1 什么是Postfix
 - 10.1.1 Postfix核心程序
 - 10.1.2 Postfix邮件队列
 - 10.1.3 Postfix工具程序
 - 10.1.4 Postfix配置文件
 - 10.1.5 Postfix查询表
 - 10.2 下载并编译Postfix
 - 10.2.1 创建Postfix用户ID和组ID
 - 10.2.2 编译Postfix
 - 10.2.3 安装Postfix
 - 10.3 配置Postfix
 - 10.3.1 编辑master.cf文件
 - 10.3.2 确定本地邮件发送方式
 - 10.3.3 编辑main.cf文件
 - 10.3.4 创建别名表
 - 10.4 启动Postfix
 - 10.5 Postfix和安全
 - 10.5.1 确定Postfix邮件丢弃安全

<<开放源码邮件系统安全>>

10.5.2 在Chroot环境中安装Postfix

10.6 小结

第11章 防止开放式转发

11.1 开放式转发和选择式转发

11.2 配置选择式转发

11.2.1 sendmail配置

11.2.2 qmail配置

11.2.3 Postfix转发参数

11.3 避免开放式转发

11.3.1 sendmail配置

11.3.2 qmail配置

11.3.3 Postfix配置

11.4 小结

第12章 阻挡垃圾邮件

12.1 阻挡垃圾邮件的方法

12.1.1 拒绝接收已知垃圾邮件主机发来的邮件

12.1.2 要求有效的SMTP信息

12.1.3 过滤垃圾邮件

12.2 垃圾邮件阻挡功能的配置

12.2.1 sendmail配置

12.2.2 qmail配置

12.2.3 Postfix配置

12.3 小结

第13章 过滤病毒

13.1 阻止病毒的方法

13.1.1 病毒过滤

13.1.2 病毒扫描

13.2 设置病毒过滤

13.3 设置病毒扫描

13.3.1 AMaViS软件

13.3.2 安装反病毒软件包

13.3.3 编译并安装AMaViS

13.3.4 为AMaViS配置MTA

13.3.5 测试病毒扫描

13.4 小结

第三部分 邮件服务安全

第14章 使用邮件防火墙

14.1 SMTP协议中的VRFY和EXPN命令

14.1.1 VRFY命令

14.1.2 EXPN命令

14.1.3 VRFY的缺陷

14.2 禁用VRFY和EXPN命令

14.2.1 sendmail

14.2.2 qmail

14.2.3 Postfix

14.3 使用邮件防火墙

14.3.1 位于网络防火墙内

<<开放源码邮件系统安全>>

- 14.3.2 位于DMZ中
- 14.3.3 作为一台内部的邮件服务器
- 14.4 创建邮件防火墙
 - 14.4.1 sendmail防火墙
 - 14.4.2 qmail防火墙
 - 14.4.3 Postfix防火墙
- 14.5 小结
- 第15章 使用SASL
 - 15.1 什么是SASL
 - 15.1.1 SASL怎样运行
 - 15.1.2 SASL认证机制
 - 15.1.3 在SMTP中使用SASL
 - 15.2 Cyrus-SASL函数库
 - 15.2.1 下载并安装Cyrus-SASL
 - 15.2.2 Cyrus-SASL数据库方法
 - 15.2.3 配置Cyrus-SASL
 - 15.3 应用SASL
 - 15.3.1 sendmail
 - 15.3.2 qmail
 - 15.3.3 Postfix
 - 15.4 测试SASL服务器
 - 15.5 小结
- 第16章 安全的POP3和IMAP服务器
 - 16.1 SSL协议族
 - 16.1.1 SSL协议
 - 16.1.2 TLS协议
 - 16.2 OpenSSL软件
 - 16.2.1 下载并编译OpenSSL
 - 16.2.2 使用证书
 - 16.3 在SSL基础上使用UW IMAP
 - 16.3.1 下载并编译UW IMAP
 - 16.3.2 为UW IMAP配置inetd进程
 - 16.3.3 测试UW IMAP
 - 16.3.4 使用网络客户端测试UW IMAP
 - 16.4 小结
- 第17章 安全的Webmail服务器
 - 17.1 什么是Webmail服务器
 - 17.1.1 TWIG
 - 17.1.2 SqWebMail
 - 17.1.3 IMHO
 - 17.1.4 WebMail
 - 17.2 TWIG Webmail服务器
 - 17.3 MySQL数据库
 - 17.3.1 使用源码形式的版本
 - 17.3.2 启动MySQL服务器
 - 17.3.3 服务器维护工作
 - 17.4 Apache Web服务器和PHP支持

<<开放源码邮件系统安全>>

- 17.4.1 下载Apache、mod_ssl和PHP
- 17.4.2 安装Apache、mod_ssl和PHP
- 17.4.3 配置Apache和PHP
- 17.4.4 测试Web服务器
- 17.5 安装TWIG Webmail服务器
 - 17.5.1 下载TWIG
 - 17.5.2 安装TWIG
 - 17.5.3 为TWIG创建MySQL数据库
 - 17.5.4 配置TWIG
 - 17.5.5 使用TWIG
- 17.6 小结

<<开放源码邮件系统安全>>

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>