

<<网络安全INTERNET 网络安全专>>

图书基本信息

书名：<<网络安全INTERNET 网络安全专业参考手册>>

13位ISBN编号：9787111063582

10位ISBN编号：7111063589

出版时间：1998-08

出版时间：机械工业出版社

作者：艾肯(美)

译者：严伟/等

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>

## 内容概要

本书是一本非常有用的网络安全手册

书籍目录

目录

序

第一部分 管理Internet安全

第1章 理解TCP/IP

1.1TCP/IP的历史

1.2探究地址、子网和主机名

1.2.1地址分类

1.2.2子网

1.2.3主机名

1.3使用网络接口

1.4网络配置文件回顾

1.4.1/etc/hosts文件

1.4.2/etc/ethers文件

1.4.3/etc/networks文件

1.4.4/etc/protocols文件

1.4.5/etc/servicecs文件

1.4.6/etc/inetd.conf文件

1.5理解网络访问文件

1.5.1/etc/hosts.equiv文件

1.5.2.rhosts文件

1.5.3用户和主机的等价性

1.6TCP/IP守护程序

1.6.1slink守护程序

1.6.2dsocket守护程序

1.6.3cpd守护程序

1.6.4行式打印机守护程序 ( 1pd )

1.6.5SNMP 守护程序 ( snm pd )

1.6.6RARP 守护程序 ( rarpd )

1.6.7BOOTP守护程序 ( bootpd )

1.6.8ROUTE守护程序 ( routed )

1.6.9域名服务守护程序 ( named )

1.6.10系统记录守护程序 ( syslogd )

1.6.11超级服务器Inetd

1.6.12RWHO守护程序 ( rwhod )

1.7使用TCP/IP实用工具

1.7.1网络管理命令

1.7.2用户命令

第2章 理解、创建守护程序

2.1什么是守护程序

2.2系统守护程序

2.2.1init守护程序

2.2.2 swapper 守护程序

2.2.3update和bdflush守护程序

2.2.41pd守护程序

2.2.51psched守护程序

2.2.6cpd和sco - cpd ( sco ) 守护程序

2.2.7cron 守护程序

2.2.8syslog守护程序

2.2.9sendmail守护程序

2.2.10getty守护程序

2.2.11rlogind守护程序

2.2.12deliver守护程序

2.2.13inetd守护程序

2.2.14routd守护程序

2.2.15 nfsd守护程序

2.2.16mountd守护程序

2.2.17pcnfsd守护程序

2.2.18statd和rpc.statd守护程序

2.2.19lockd和rpc.lockd守护程序

2.3用BourneShell创建守护程序

2.3.1处理入境和输出

2.3.2 处理消息

2.3.3处理信号

2.3.4dfmon 程序

2.4用PERL创建守护程序

2.4.1处理入境和输出

2.4.2 处理信号

2.4.3procmon 程序

2.5Unix运行级别

2.6 程序清单

2.6.1程序清单2.1 dfmon程序

2.6.2程序清单2.2 dfmon的

配置文件

2.6.3程序清单2.3 procmon

命令

2.6.4程序清单2.4 procmon .cfg

文件

第3章 使用UUCP

3.1UUCP的历史

3.2 UUCP网络

3.3为主机命名

3.4系统V基本网络实用工具UUCP

3.4.1UUCP文件布局

3.4.2配置UUCP

3.4.3测试连接

3.4.4Dialers文件

3.4.5系统文件

3.5UUCP交谈脚本

3.5.1使用uucico测试连接

3.5.2权限文件

3.5.3允许匿名UUCP访问

3.5.4UUCP 日志文件

3.5.5维护

3.6配置版本2UUCP

3.6.1版本2UUCP是什么

3.6.2文件布局

3.6.3配置UUCP

3.6.4L - devices文件

3.6.5 测试连接

3.6.6 L.sys文件

3.6.7用uucico测试连接

3.6.8版本2权限

3.6.9日志文件

3.6.10 维护

3.7 在TCP/IP之上配置UUCP

3.8代码清单

3.8.1代码清单3.1 gtimes.c

3.8.2代码清单3.2 genUSER

第4章 审计跟踪

4.1Unix系统的审计跟踪

4.1.1一般的Unix日志

4.1.2进程记帐

4.1.3审计中有用的工具

4.1.4 其他可以联机使用的报告  
工具

4.2WindowsNT的审计跟踪

4.2.1使用事件查看器

4.2.2记录ftp服务器的服务

4.2.3记录httpd事务

4.2.4用WindowsNT的其他TCP/IP

应用程序记录

4.3DOS下的审计跟踪

4.3.1PC/DACS

4.3.2Watchdog

4.3.3LOCK

4.4使用SystemLog发现入侵者

4.4.1一般入侵提示

4.4.2 潜在的问题

第二部分 访问并且保护网关

第5章 IP欺骗与窥探

5.1窥探

5.1.1窥探：如何实施

5.1.2窥探：如何威胁安全

5.1.3协议窥探：一个案例学习  
( casestudy )

5.1.4窥探：如何预防

5.1.5硬件障碍

5.1.6避免传输口令

## 5.2 欺骗

### 5.2.1 硬件地址欺骗

### 5.2.2 ARP欺骗

### 5.2.3 防止ARP欺骗

### 5.2.4 窥探案例学习再讨论

### 5.2.5 检测ARP欺骗

### 5.2.6 欺骗IP路由系统

### 5.2.7 基于ICMP的路由欺骗

### 5.2.8 误导IP数据报

### 5.2.9 防止路由欺骗

### 5.2.10 案例学习：涉及外部路由

### 5.2.11 欺骗域名系统的名字

### 5.2.12 欺骗TCP连接

## 第6章 如何构造防火墙

### 6.1 TIS防火墙工具箱

#### 6.1.1 理解TIS防火墙工具箱

#### 6.1.2 如何获得TIS防火墙工具箱

#### 6.1.3 在SunOS4.1.3及4.1.4下 编译

#### 6.1.4 在BSDI下编译

#### 6.1.5 安装TIS防火墙工具箱

### 6.2 准备配置

### 6.3 配置TCP/IP

### 6.4 netperm表

### 6.5 配置netac1

#### 6.5.1 与netacl连接

#### 6.5.2 重新启动inetd

### 6.6 配置Telnet代理

#### 6.6.1 通过Telnet代理建立连接

#### 6.6.2 主机访问规则

#### 6.6.3 检测Telnet代理

### 6.7 配置rlogin网关

#### 6.7.1 经rlogin网关建立连接

#### 6.7.2 主机访问规则

#### 6.7.3 检测rlogin代理

### 6.8 配置FTP网关

#### 6.8.1 主机访问规则

#### 6.8.2 检测FTP代理

#### 6.8.3 通过FTP代理建立连接

#### 6.8.4 允许FTP

### 6.9 配置serndmail代理：smap和 smapd

#### 6.9.1 安装smap客户程序

#### 6.9.2 配置smap客户

#### 6.9.3 安装smapd应用程序

#### 6.9.4 配置smapd应用程序

#### 6.9.5 为smap 配置DNS

<<网络安全INTERNET 网络安全专>>

6.10配置HTTP代理

6.10.1非代理意识HTTP客户

6.10.2使用代理意识HTTP客户

6.10.3主机访问规则

6.11配置X窗口代理

6.12理解认证服务器

6.12.1认证数据库

6.12.2添加用户

6.12.3认证Shell authmgr

6.12.4数据库管理

6.12.5认证如何工作

6.13其他服务使用plug - gw

6.13.1配置plug - gw

6.13.2plug - gw与NNTP

6.13.3plug - gw与POP

6.14管理工具

6.14.1portscan

6.14.2netscan

6.14.3报告工具

6.15何处寻求帮助

6.16netpem - table文件示例

6.17参考手册

6.17.1Authmgr 网络认证客户

程序

6.17.2authsrv 第三方网络认证守

护程序

6.17.3ftp - gw FTP代理服务器

6.17.4http - gw Gopher/HTTP

代理

6.17.5login - sh 认证登录shell

6.17.6netacl TCP网络访问

控制

6.17.7plug - gw 通用TCP插接板

(plug - board)代理

6.17.8rlogin - gw rlogin代理

服务器

6.17.9smmap sendmail包装(wrapper)

客户

6.17.10smmapd sendmail1包装守

护程序

6.17.11tn - gw telnet代理服务

器

6.17.12x - gw X网关服务器

第7章如何购买防火墙

7.1防火墙回顾

7.1.1体系结构

7.1.2应了解的三个术语

- 7.2选择防火墙
- 7.3防火墙体系结构
  - 7.3.1路由器体系
  - 7.3.2先进防火墙体系
- 7.4评估防火墙
  - 7.4.1选择状态包过滤器或传输防火墙
  - 7.4.2评估通过防火墙的路径
  - 7.4.3评估管理接口和GUI
  - 7.4.4评估灵活性和特征
  - 7.4.5评估报告和记帐
- 7.5评估防火墙性能
  - 7.5.1包过滤性能问题
  - 7.5.2传输代理性能问题
  - 7.5.3性能测试规则
- 7.6评估防火墙的安全
- 7.7总结
- 第8章 SATAN与Internet
  - 8.1网络攻击的本质
    - 8.1.1Internet威胁层 (ITL)
    - 8.1.2普通攻击方法
    - 8.1.3安全漏洞概述
    - 8.1.4 学习新的安全漏洞
  - 8.2像入侵者那样思考
    - 8.2.1收集系统信息
    - 8.2.2掌握代码
    - 8.2.3尝试所有已知问题
    - 8.2.4漏洞与机会匹配
    - 8.2.5查找弱连接
    - 8.2.6总结远程网络攻击
    - 8.2.7自动搜索
  - 8.3初次遭遇SATAN
    - 8.3.1历史
    - 8.3.2创造者
    - 8.3.3与其他工具的比较
    - 8.3.4厂商反应
    - 8.3.5长期影响
  - 8.4检测SATAN
    - 8.4.1Courtney
    - 8.4.2Gabriel
    - 8.4.3TCPWrappers
    - 8.4.4netlog/TAMU
    - 8.4.5 Argus
  - 8.5使用安全的网络程序
    - 8.5.1Kerberos
    - 8.5.2安全Shell (ssh)
  - 8.6 SSL



## 8.7研究SATAN做什么

### 8.7.1SATAN的信息收集

### 8.7.2搜索的脆弱点

### 8.7.3其他网络脆弱点

### 8.7.4探讨IP欺骗

### 8.7.5检验结构型Internet问题

## 8.8SATAN集结

### 8.8.1 获取SATAN

### 8.8.2检查SATAN文件

## 8.9 构造SATAN

### 8.9.1使用SATAN HTML 界面

### 8.9.2运行一个扫描

### 8.9.3理解SATAN数据库记录格式

### 8.9.4理解SATAN规则集

### 8.9.5扩展SATAN

### 8.9.6使用SATAN的长期利益

## 8.10引用文献

## 第9章 Kerberos

### 9.1Kerberos如何工作

### 9.2Kerberos网络

#### 9.2.1RFC

#### 9.2.2Kerberos的目标

### 9.3认证如何工作

### 9.4 加密

#### 9.4.1私有、公开、秘密或共享密 钥加密

#### 9.4.2私人或私密密钥加密

#### 9.4.3DES及其变体

#### 9.4.4加密出口问题

#### 9.4.5加密和校验和规范

### 9.5Kerberos版本

#### 9.5.1不同的Kerberos版本4

#### 9.5.2不同的Kerberos版本5

#### 9.5.3Bones

### 9.6选择销售商

### 9.7销售商的互操作性问题

#### 9.7.1DECULTRIXKerberos

#### 9.7.2Transarc的Kerberos

#### 9.7.3DCE

#### 9.7.4互操作性要求

### 9.8命名约束 (namingconstraints)

#### 9.8.1区域名

#### 9.8.2主体名字

### 9.9跨区域 (Cross - Realm) 操作

### 9.10 ticket标志

#### 9.10.1初始及预认证ticket

#### 9.10.2无效ticket

- 9.10.3可更新的ticket
  - 9.10.4过期ticket
  - 9.10.5可代理的及代理ticket
  - 9.10.6可转发的ticket
  - 9.10.7认证标志
  - 9.10.8其他密钥分配中心选项
  - 9.11消息交换
    - 9.11.1ticket与认证符
    - 9.11.2认证服务交换
    - 9.11.3TicketGranting Service ( TGS ) 交换
    - 9.11.4认证服务器与TicketGranting Service交换规范
    - 9.11.5客户/服务器认证交换
    - 9.11.6客户/服务器 ( CS ) 消息规范
    - 9.11.7KRB \_\_SAFE交换
    - 9.11.8KRB \_\_SAFE消息规范
    - 9.11.9KRB \_\_PRIV交换
    - 9.11.10 KRB \_\_PRIV消息规范
    - 9.11.11KRB \_\_CRED 交换
    - 9.11.12KRB \_\_CRED 消息规范
    - 9.11.13名字
    - 9.11.14时间
    - 9.11.15主机地址
    - 9.11.16授权数据
    - 9.11.17最后请求数据
    - 9.11.18 错误消息规范
  - 9.12 Kerberos工作站认证问题
    - 9.12.1Kerberos的端口号
    - 9.12.2Kerberos的Telnet
    - 9.12.3Kerberosftpd
  - 9.13其他信息源
- 第三部分 消息机制：创建安全的通道
- 第10章 加密概述
- 10.1加密技术概述
  - 10.2密码术语
  - 10.3密码技术的应用
    - 10.3.1黑客和窃贼的威胁
    - 10.3.2密码技术的目标
    - 10.3.3数字ID，证明和证明机构 ( certificateauthority )
    - 10.3.4数字签名
    - 10.3.5网络登录和认证的安全性
    - 10.3.6安全通道
    - 10.3.7安全Internet隧道
    - 10.3.8 电子商务

## 10.4对称（私钥）密码技术

### 10.4.1转置

### 10.4.2解密

### 10.4.3置换

### 10.4.4块密码和流密码

### 10.4.5DES（数据加密标准）

### 10.4.6DES的其他替代选择

### 10.4.7Blowf ish

## 10.5非对称（公钥）密码技术

### 10.6攻击和密码学分析

### 10.7有关密码技术的地址

### 10.8小结

## 第11章 PGP程序

### 11.1PGP 概述

#### 11.1.1PGP的历史

#### 11.1.2为什么要使用PGP

#### 11.1.3加密简短回顾

### 11.2 PGP的使用

#### 11.2.1在使用PGP之前

#### 11.2.2 产生一个PGP密钥

#### 11.2.3公钥的发布

#### 11.2.4 为一个消息签名

#### 11.2.5添加其他人的密钥

#### 11.2.6加密一个消息

#### 11.2.7解密和验证消息

### 11.3PGP密钥

#### 11.3.1名字中是什么

#### 11.3.2PGP密钥环

#### 11.3.3Web的受托性

#### 11.3.4信任程度

### 11.4密钥管理

#### 11.4.1密钥产生

#### 11.4.2向公钥环中添加密钥

#### 11.4.3从公钥环中提取密钥

#### 11.4.4为密钥签名

#### 11.4.5查看密钥环的内容

#### 11.4.6 删除密钥和签名

#### 11.4.7密钥指纹和验证密钥

#### 11.4.8取消你的密钥

### 11.5基本消息操作

#### 11.5.1PGP是程序还是过滤器

#### 11.5.2 压缩消息

#### 11.5.3处理文本和二进制文件

#### 11.5.4通过电子邮件发送PGP消息

#### 11.5.5常规加密

#### 11.5.6为一个消息签名

#### 11.5.7用公钥加密消息

- 11.5.8为一个消息签名和加密
- 11.5.9消息的解密和验证
- 11.6高级消息操作
  - 11.6.1净签
  - 11.6.2分离签名
  - 11.6.3For Her EyesOnly
  - 11.6.4清除文件
- 11.7PGP配置文件
- 11.8PGP的安全性
  - 11.8.1蛮力攻击
  - 11.8.2 私钥和通过短语
  - 11.8.3对公钥环的攻击
  - 11.8.4程序的安全性
  - 11.8.5对PGP的其他攻击
- 11.9 PGP的扩充
  - 11.9.1PGP公钥服务器
  - 11.9.2PGPMenu : PGPforUnix的菜单界面
  - 11.9.3Windows前端
  - 11.9.4Unix邮件程序
  - 11.9.5MacPGP
- 第四部分 当前关注的问题
- 第12章 Wind0ws NT的Internet安全
  - 12.1WindowsNT概述
  - 12.2WindowsNT操作环境
    - 12.2.1域
    - 12.2.2用户帐户、组、权利和权限
  - 12.3WindowsNT的登录和认证
  - 12.4WindowsNT中与Intranet有关的特性
    - 12.4.1在Intranet中使用DNS服务器
    - 12.4.2在Intranet中使用NetBIOS名字转换
    - 12.4.3在Intranet中使用WINS服务器
  - 12.5连接到Internet上的考虑
    - 12.5.1使用IIS的公共Web服务器连接
    - 12.5.2代理服务器连接
    - 12.5.3在WindowsNT中配置服务
    - 12.5.4在WindowsNT中配置端口
  - 12.6MicrosoftInternetInformation Server
  - 12.7Microsoft代理服务器
  - 12.8新的WindowsNT目录服务模型

## 12.9总结

## 第13章 Java的安全性

### 13.1Java 的功能

#### 13.1.1Java是可移植的

#### 13.1.2Java 是健壮的

#### 13.1.3Java 是安全的

#### 13.1.4Java 是面向对象的

#### 13.1.5Java是高性能的

#### 13.1.6Java 是容易使用的

### 13.2Java语言的历史

### 13.3Java环境的主要功能特性

#### 13.3.1Java语言的特性

#### 13.3.2Java 体系结构

### 13.4从类文件到执行

#### 13.4.1代码的编译

#### 13.4.2运行代码

### 13.5Java虚拟机

#### 13.5.1要建立一个新的机器代码规范

#### 13.5.2Java 虚拟机描述

### 13.6设置Java 安全性功能

#### 13.6.1使用App letv ewer

#### 13.6.2Netscape3.0

#### 13.6.3使用Java 程序的其他方面问题

## 第14章 CGI安全性

### 14.1CGI接口介绍

#### 14.1.1为什么CGI是危险的

#### 14.1.2CGI如何工作

#### 14.1.3CGI数据：编码和解码

#### 14.1.4CGI库

### 14.2理解CGI的脆弱性

#### 14.2.1HTTP服务器

#### 14.2.2HTTP协议

#### 14.2.3环境变量

#### 14.2.4GET和POST输入数据

### 14.3尽量减小CGI的脆弱性

#### 14.3.1限制对CGI的访问

#### 14.3.2用最小的特权运行CGI

#### 14.3.3在一个改变根文件系统的环境中运行

#### 14.3.4保护HTTP服务器所在的机器

### 14.4CGIWRAP：另一种模型

### 14.5越过CGI

### 14.6服务器方包含 ( SSI )

#### 14.6.1限制对SSI的访问

<<网络安全INTERNET 网络安全专>>

- 14.6.2SSI的替代
- 14.7语言问题
  - 14.7.1PERL
  - 14.7.2C和C + 十
  - 14.7.3安全语言
- 14.8保护敏感数据
- 14.9日志记录
- 第15章 病毒
  - 15.1用户的角度
  - 15.2 什么是计算机病毒
  - 15.3最可能的目标
    - 15.3.1关键硬件
    - 15.3.2关键软件
    - 15.3.3软引导记录 ( FBR )
    - 15.3.4硬盘主引导记录
    - 15.3.5分区引导记录
    - 15.3.6系统服务
    - 15.3.7程序文件
    - 15.3.8带有宏能力的数据文件
  - 15.4IBMPC计算机的病毒类型
    - 15.4.1引导记录病毒
    - 15.4.2软引导记录病毒
    - 15.4.3分区引导记录病毒
    - 15.4.4主引导记录病毒
    - 15.4.5程序文件病毒
    - 15.4.6伙伴病毒
    - 15.4.7文件感染病毒的潜在破坏
    - 15.4.8宏病毒
    - 15.4.9 蠕虫
  - 15.5网络和Internet对病毒的敏感性
    - 15.5.1网络对文件病毒的敏感性
    - 15.5.2 引导病毒
    - 15.5.3宏病毒
  - 15.6病毒类型
    - 15.6.1多态病毒
    - 15.6.2Stealth病毒
    - 15.6.3Slow 病毒
    - 15.6.4Retro病毒
    - 15.6.5多头病毒 ( Multipartite Viruses )
  - 15.7反病毒程序如何工作
    - 15.7.1病毒扫描程序
    - 15.7.2 内存扫描程序
    - 15.7.3完整性检查器
    - 15.7.4行为阻止者
    - 15.7.5启发式扫描器
  - 15.8预防措施和治疗

15.8.1防止和修复引导记录病毒

15.8.2防止和修复可执行文件病毒

15.8.3修复读取隐藏病毒感染的文件

15.8.4防止和修复宏病毒

15.9WindowsNT下病毒行为概况

15.9.1WindowsNT下的主引导记录病毒

15.9.2WindowsNT下的引导记录病毒

15.9.3 Windows NT DOS框内的DOS文件病毒

15.9.4WindowsNT下的Windows 3.1病毒

15.9.5WindowsNT下的宏病毒

15.9.6本机的WindowsNT病毒

15.10总结

第五部分 附录

附录A 安全性信息来源

附录BInternet安全性索引

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>