ICSA 国家信息中心 启明星辰公司 策划

UNIX 系统安全

启明星辰公司
高鹏 严望佳 编著

计算机网络安全系列丛书

清华大学出版社
http://www.tup.tsinghua.edu.cn

计算机网络安全系列丛书

UNIX 系统安全

启明星辰公司
高鹏　严望佳　编著

清华大学出版社

(京)新登字158号

内 容 简 介

UNIX是一个优秀的操作系统，功能强大、性能稳定、配置灵活。但用户在实际配置UNIX系统时，经常忽略一个重要的问题——安全问题；或者用户不了解如何配置一个安全的UNIX系统。本书用来帮助用户解决UNIX的安全问题。

它不仅仅是讲述UNIX安全的书，还是一本很好的UNIX配置方法教材。读者不仅可以从中掌握UNIX的安全性，还可以通过学习UNIX的安全更加深入地掌握UNIX系统。

本书适合于对UNIX系统有初步经验的计算机用户。对于没有UNIX基础的读者，在阅读前几章后，同样可以理解本书的精髓。

书　　名：UNIX 系统安全
作　　者：启明星辰公司　高鹏　严望佳
出 版 者：清华大学出版社(北京清华大学校内，邮编 100084)
http://www.tup.tsinghua.edu.cn
责任编辑：王鉴莉
印 刷 者：北京市清华园胶印厂
发 行 者：新华书店总店北京发行所
开　　本：787×1092 1/16　**印张**：17.75　**字数**：314 千字
版　　次：1999 年 6 月第 1 版　1999 年 10 月第 2 次印刷
书　　号：ISBN 7-302-03515-6/TP・1923
印　　数：5001～10000
定　　价：29.00 元

谨以此书献给我们的老师

严望佳

丛 书 序

全球信息高速公路的建设，Internet/Intranet 的发展，将对整个社会的科学与技术、经济与文化带来巨大的推动与冲击，同时也给我们带来了许多的挑战。Internet/Intranet 信息安全是一个综合的系统工程，需要我们在网络安全技术的研究和应用领域做长期的攻关和规划。

在 Internet/Intranet 的大量应用中，Internet/Intranet 安全面临着重大挑战。事实上，资源共享和信息安全历来是一对矛盾。近年来随着 Internet 的飞速发展，计算机网络的资源共享进一步加强，随之而来的信息安全问题日益突出。据美国 FBI 统计，美国每年因网络安全问题所造成的经济损失高达 75 亿美元。而全球平均每 20 秒钟就发生一起 Internet 计算机侵入事件。

一般认为，计算机网络系统的安全威胁主要来自黑客攻击、计算机病毒和拒绝服务攻击 3 个方面。目前，人们也开始重视来自网络内部的安全威胁。

黑客攻击早在主机终端时代就已经出现，随着 Internet 的发展，现代黑客则从以系统为主的攻击转变到以网络为主的攻击。新的手法包括：通过网络监听获取网上用户的帐号和密码；监听密钥分配过程，攻击密钥管理服务器，得到密钥或认证码，从而取得合法资格；利用 UNIX 操作系统提供的守护进程的缺省帐户进行攻击，如 Telnet Daemon、FTP Daemon 和 RPC Daemon 等；利用 Finger 等命令收集信息，提高自己的攻击能力；利用 SendMail，采用 debug、wizard 和 pipe 等进行攻击；利用 FTP，采用匿名用户访问进行攻击；利用 NFS 进行攻击；通过隐蔽通道进行非法活动；突破防火墙等等。目前，已知的黑客攻击手段多达 500 余种。

计算机病毒与“蠕虫”程序有所不同，它们主要的区别是，“蠕虫”寄生于操作系统之上，而计算机病毒寄生于一般的可执行程序上。计算机病毒种类繁多，极易传播，影响范围广。它动辄删除、修改文件，导致程序运行错误，甚至死机，已构成对 Internet/Intranet 的严重威胁。

拒绝服务攻击是一种破坏性攻击，最早的拒绝服务攻击是“电子邮件炸弹”。它的表现形式是用户在很短的时间内收到大量无用的电子邮件，从而影响正常业务的运行。严重时会使系统关机、网络瘫痪。

总而言之，对 Internet/Intranet 安全构成的威胁可以分为以下若干类型：黑客入侵、来自内部的攻击、计算机病毒的侵入、秘密信息的泄漏和修改网络的关键数据等，这些都可以造成 Internet 瘫痪或引起 Internet 商业的经济损失等等。人们面临的计算机网络系统的安全威胁日益严重。

黑客攻击等威胁行为为什么能够经常得逞呢？主要原因在于 Internet/Intranet 系统内在安全的脆弱性；其次是人们思想麻痹，没有正视黑客入侵所造成的严重后果，因而舍不得投入必要的人力、财力和物力来加强 Internet/Intranet 的安全性，没有采取有效的安全策略和安全机制。另外，缺乏先进的网络安全技术、工具、手段和产品等原因，也导致网络的安全防范能力差。

由于我国网络研究起步晚，网络安全技术还有待整体的提高和发展。我很高兴看到这套丛书的诞生，该丛书系统全面地介绍了计算机网络安全各方面的问题，并且从一些新的角度进行探讨，例如，如何针对 Internet/Intranet 系统的安全威胁建立正确的安全策略；如何提出 Internet/Intranet 系统安全的整体解决方案；如何严格规范建立 Internet/Intranet 系统的安全机制等。这对提高我国网络安全防范能力将有重要的参考作用。

这套由国家信息中心、国际计算机安全协会(ICSA)以及启明星辰信息技术有限公司(Vtech)策划的网络安全系列丛书具有起点高、技术覆盖面广等特点。包括了对业界最新的网络安全技术、操作系统漏洞和防范方法、网络安全工具以及黑客攻击手段等的详细分析和介绍。读者可以带着各种问题、从不同的角度来了解这些技术，一定会有所收获。

中国工程院院士　沈昌祥

前　言

计算机的安全问题越来越引起世界各国的关注，这也是一个十分复杂的课题。随着计算机在人类生活各领域中的广泛应用，计算机病毒在不断产生和传播，计算机网络不断被非法入侵、重要情报资料被窃取、甚至导致网络系统的瘫痪等诸多问题，已给各个国家以及众多公司造成巨大的经济损失，甚至危害到国家和地区的安全。因此计算机系统的安全问题是一个关系到人类生存与发展的大事情，必须充分重视并设法解决。

本书的目的是介绍并深入论述 UNIX 系统的安全问题，主要从 UNIX 网络安全(尤其是 Internet 上的网络安全)展开，使读者在读完本书后能掌握构建一个更安全的 UNIX 系统的方法。在此基础上，本书还介绍一些实用的 UNIX 系统安全的工具。

一、读者对象

本书面向的读者是具有初步 UNIX 系统管理经验，对 TCP/IP 协议有一定的了解，并能对 UNIX 网络进行基本配置的用户。对于不熟悉 UNIX 系统的用户，在阅读前几章后也同样可以从本书中受益。本书首先介绍有关 UNIX 系统安全方面的一些基本概念，之后逐步深入。

二、本书结构

本书可分为如下几个部分：

第一部分包括第一和第二章，简要介绍网络安全的相关概念，并在此基础上论述如何对现有的系统做安全规划。

此外，还介绍信息系统存在的安全方面的问题，尤其针对 UNIX 系统讲述其存在的一些安全脆弱性。

第二部分包括第三章，介绍与 UNIX 系统的安全相关的基本概念。

第三部分包括第四和第五章，介绍以黑客(hacker)的身份，通过攻击一个 UNIX 系统来检验现有系统的安全性，并有针对性地讲述如何提高 UNIX 系统

的安全性。

第四部分包括第六、第七和第八章，介绍网络安全工具和 UNIX 系统已知的安全漏洞，以及在系统被攻破后应该采取的措施等。

附录部分，介绍能提高系统安全性的一些实用工具软件，以及配置 UNIX 系统时常用的命令程序。

阅读本书之后，读者能够在对 UNIX 系统进行维护的时候，提高对系统安全方面的认识；并能利用本书提供的 UNIX 系统安全配置方法，再以用户自己具体的 UNIX 系统作为参照，使系统变得更加安全、可靠；还可以利用本书推荐的安全工具，提高 UNIX 系统的安全性。

这套丛书的策划和出版得到以下朋友的热情支持和帮助，谨在这里表示我们诚挚的谢意：中国信息安全专业委员会李正男主任、刘世键主任、吴亚飞秘书长，中国信息大学执行董事刘建国先生，国家信息大学信息安全处叶红、董小玲、张翔和孙卫红，美国格莱瑞技术公司严立。

目　录

第一章　网络安全概述 1

1.1　网络安全简介 2
1.2　历史事故 2
1.3　因特网上的 FBI 6
1.4　网络安全的重要性 6
1.5　计算机安全的正式分级 8
1.6　信息系统安全的脆弱性 11
1.6.1　操作系统安全的脆弱性 12
1.6.2　计算机网络安全的脆弱性 13
1.6.3　数据库管理系统安全的脆弱性 13
1.6.4　缺少安全管理 13
1.7　UNIX 网络不安全的因素 13
1.7.1　特权软件的安全漏洞 14
1.7.2　研究源代码的漏洞 16
1.7.3　特洛伊木马 16
1.7.4　网络监听及数据截取 17
1.7.5　软件之间相互作用和设置 17
1.8　安全控制的种类 18
1.8.1　内部控制 18
1.8.2　外部控制 18
1.8.3　内部和外部控制相结合 19
1.9　网络安全的方法 19
1.9.1　允许访问 19
1.9.2　拒绝访问 20
1.9.3　异常处理 20

第二章　网络安全策略 21

2.1　层次模型 22
2.2　特定层次中的防火墙模型 23

2.3 局域网内部的计算机 …… 25
2.4 安全规划 …… 27
2.5 威胁评估 …… 27
2.6 分布式控制 …… 28
2.7 使用子网去分散控制 …… 29
2.8 使用邮址表分发信息 …… 29
2.9 编写安全策略文件 …… 30
2.9.1 检查登录活动 …… 31
2.9.2 COPS 程序包 …… 33
2.9.3 限制访问权 …… 35
2.9.4 加密 …… 35
2.9.5 防火墙 …… 37
2.9.6 Wrapper 程序 …… 41
第三章 UNIX 系统安全入门 …… 45
3.1 UNIX 系统的基本知识 …… 46
3.1.1 网络配置文件 …… 46
3.1.2 TCP/IP 守护进程 …… 48
3.2 普通用户的安全 …… 51
3.2.1 口令安全 …… 51
3.2.2 文件许可权 …… 52
3.2.3 目录许可 …… 53
3.2.4 umask 命令 …… 53
3.2.5 设置用户 ID 和同组用户 ID 许可 …… 53
3.2.6 cp、mv、ln 和 cpio 命令 …… 54
3.2.7 su 和 newgrp 命令 …… 55
3.2.8 文件加密 …… 55
3.2.9 其他的安全问题 …… 56
3.3 程序员的安全性考虑 …… 56
3.3.1 系统调用 …… 57
3.3.2 标准 C 库 …… 60
3.4 超级用户的安全 …… 62
3.4.1 超级用户 …… 62
3.4.2 安全管理 …… 63
3.4.3 文件系统安全 …… 63
第四章 已知的 UNIX 漏洞的解决方法 …… 69
4.1 SunOS 上的漏洞 …… 70

4.1.1 arp 问题 ····· 70
4.1.2 GNU in.fingerd 问题 ····· 70
4.1.3 lpd 问题 ····· 72
4.1.4 mountd 问题 ····· 72
4.1.5 nfsd 问题 ····· 73
4.1.6 passwd 问题 ····· 74
4.1.7 RPC 问题 ····· 81
4.1.8 sunsrc 问题 ····· 81
4.2 HP-UX 系统的漏洞 ····· 82
4.2.1 chfn 问题 ····· 82
4.2.2 /system/PHxx_nnnn 问题 ····· 82
4.2.3 Xauthority 问题 ····· 83
4.3 libc-4.6.27 问题 ····· 83
4.4 at 命令问题 ····· 84
4.5 网络监听 ····· 87
4.6 telnet 问题 ····· 91
4.7 dip 命令问题 ····· 94
4.8 tcp_syn_flooding ····· 95
4.9 sendmail 漏洞 ····· 96
4.10 passwd 命令漏洞 ····· 99
4.11 yppasswd 漏洞 ····· 103
4.12 ping 命令问题 ····· 104
第五章 以网络黑客的身份检查 UNIX 系统的安全性 ····· 109
5.1 开始攻击系统 ····· 110
5.2 用 FTP 攻击系统实例 ····· 113
5.3 利用 RPC 攻击系统实例 ····· 117
5.4 通过 X Window 攻击系统的方法 ····· 120
5.5 利用 sendmail 攻击系统实例 ····· 121
5.6 信任关系 ····· 124
第六章 提高 UNIX 安全的方法 ····· 125
6.1 补丁程序 ····· 126
6.2 网络安全措施 ····· 126
6.2.1 服务过滤 ····· 126
6.2.2 r 命令 ····· 127
6.2.3 /etc/hosts.equiv 文件 ····· 128
6.2.4 /etc/netgroup 文件 ····· 128

6.2.5 $HOME/.rhosts 文件 129
6.2.6 NFS 129
6.2.7 /etc/hosts.lpd 文件 131
6.2.8 安全的终端设置 131
6.2.9 网络服务安全 131
6.2.10 portmapper 服务 132
6.2.11 trivial ftp (tftp)服务 132
6.2.12 /etc/services 文件 132
6.2.13 TCP_Wrapper 程序包 133
6.2.14 /etc/aliases 文件 133
6.2.15 打开 NFS 端口监视功能 133
6.2.16 ypbind 134
6.2.17 IP forwarding 134
6.2.18 系统核心的修改 135
6.2.19 文件/etc/ftpusers 135
6.2.20 在文件系统 fsirand 上安装随机数 i 节点生成器 136
6.2.21 在加载文件系统时使用 nosuid 选项 136
6.2.22 文件/etc/ttytab 137
6.2.23 eeprom 的安全域 137
6.2.24 文件/dev/eeprom 的访问权限 137
6.2.25 去掉 openprom 支持 137
6.2.26 文件/etc/fbtab 138
6.2.27 文件/etc/rc 和$HOME/.login 138
6.2.28 目录/etc 下的文件 138
6.2.29 去掉用户的 setuid 属性 139
6.2.30 去掉工作组的 setgid 属性 140
6.2.31 更改配置文件/etc/syslog.conf 140
6.2.32 核心文件的权限 140
6.2.33 使用 sendmail 服务 141
6.2.34 fingerd 服务 142
6.2.35 UUCP 142
6.2.36 rexd 服务 142
6.2.37 httpd 服务 143
6.3 FTP 和匿名 FTP 144
6.3.1 版本 144
6.3.2 匿名 FTP 的安全性 144
6.4 口令和帐号安全 147

6.4.1 口令安全策略 148
6.4.2 Proactive Checking 148
6.4.3 NIS、NIS+和/etc/passwd 中的记录项 148
6.4.4 password shadow 149
6.4.5 系统管理 149
6.4.6 特殊帐号 149
6.4.7 root 帐号 150
6.4.8 .netrc 文件 150
6.4.9 GCOS 域 151
6.5 文件系统安全 151
6.5.1 概述 151
6.5.2 启动和关闭系统的脚本文件 151
6.5.3 /usr/lib/expreserve 文件 152
6.5.4 外部文件系统/设备 152
6.5.5 文件访问权限 152
6.5.6 由 root 运行的文件 153
6.5.7 bin 所有权限 153
6.5.8 Tiger/COPS 安全工具 154
6.5.9 Tripwire 安全工具 154
6.6 X Window 的安全性 154
6.6.1 X Window 安全入门 154
6.6.2 网络黑客通过 X Window 的漏洞可以做的破坏 155
6.6.3 提高 X Window 的安全性的方法 155
6.6.4 xterm 的不安全因素 157
6.6.5 xdm 的问题 158
6.7 IP 欺骗技术攻击方法 158
6.8 NIS 系统的安全性 159
6.8.1 NIS 结构 160
6.8.2 NIS 安全脆弱性 161
6.8.3 攻击 NIS 的例子 162
6.8.4 可能的解决方法 163
6.9 特定 UNIX 操作系统的安全 163
6.9.1 SunOS 4.1.x 163
6.9.2 Solaris 2.x 167
6.9.3 IRIX 169
6.9.4 AIX 169
6.9.5 HP/UX 169

6.9.6 OSF 170
6.9.7 Ultrix 170
第七章 UNIX 网络安全工具 173
7.1 加密工具 174
7.1.1 Kerberos 174
7.1.2 DES 175
7.1.3 MD2、MD4 和 MD5 176
7.1.4 SSH 177
7.2 安全评定工具 182
7.2.1 SATAN 190
7.2.2 ISS 196
7.2.3 Strobe 工具 203
7.2.4 COPS 205
7.2.5 NSS 208
7.2.6 Chkacct v1.1 209
7.2.7 Tripwire 210
7.3 网络监听工具 213
7.3.1 网络监听的概念 213
7.3.2 网络监听的作用 216
7.3.3 snoop 219
7.3.4 Sniffit 软件 220
7.3.5 其他网络监听工具 225
7.3.6 Argus 226
7.3.7 ARP Monitor 226
7.3.8 arpwatch1.3 227
7.3.9 Courney 227
7.3.10 Hobgoblin 227
7.3.11 md5check 228
7.3.12 NetMan 228
7.3.13 nfswatch 228
7.3.14 NID 228
7.3.15 NOCOL 228
7.3.16 noshell 229
7.3.17 Raudit 229
7.3.18 Swatch 299
7.3.19 swIPE 230
7.3.20 TAMU Check Integrity Script 230

7.3.21 Watcher ····· 230
7.3.22 X Connection Monitor ····· 230
7.3.23 ident ····· 231
7.3.24 ifstatus ····· 231
7.3.25 lsof ····· 232
7.4 口令安全工具 ····· 232
7.4.1 npasswd ····· 232
7.4.2 checkpasswd ····· 232
7.4.3 Cracklib ····· 233
7.4.4 yppapasswd ····· 235
7.4.5 Alec Muffett 的 Crack ····· 235
7.5 安全提升工具 ····· 236
7.5.1 TCP_Wrapper ····· 236
7.5.2 cpm ····· 237
7.5.3 Smrsh ····· 237
7.5.4 rscan ····· 240
7.5.5 logdaemon ····· 240
7.5.6 portmapper/rpcbind ····· 240
7.5.7 PGP ····· 241
7.5.8 chrootuid ····· 241
7.5.9 CGIWRAP ····· 241
7.5.10 Washington University ftpd (wu-ftpd) ····· 241
7.5.11 Anonymous FTP Configuration Guidelines ····· 242
7.5.12 Token Generators ····· 242
7.5.13 S/Key ····· 242

第八章 系统安全状态的检查及攻破后的措施 ····· 245

8.1 查看系统是否已被侵入的方法 ····· 246
8.1.1 日志文件 ····· 246
8.1.2 setuid 文件和 setgid 文件 ····· 247
8.1.3 查看系统的二进制文件是否被更改 ····· 247
8.1.4 检查所有由 cron 和 at 运行的文件 ····· 248
8.1.5 检查系统上不正常的隐藏文件 ····· 248
8.1.6 检查局域网上的每台机器 ····· 248
8.1.7 检查文件/etc/passwd 是否被修改 ····· 248
8.1.8 检查系统网络配置中非法的项 ····· 249
8.1.9 检查是否有网络监听程序在运行 ····· 249
8.1.10 检查系统上的非正常的隐藏文件 ····· 249

8.2 系统被攻破后应采取的措施 250
8.2.1 查找入侵者的来源 250
8.2.2 检查系统上的一些关键二进制文件 251
8.2.3 对用户帐号下的文件进行检查 252
8.2.4 NFS 252
8.2.5 恢复控制 252
8.2.6 分析入侵方式 253
8.2.7 恢复正常 254
8.2.8 提高系统的安全性的方法 255
附录 A 从 Internet 上获取免费的安全方面的资料 256
附录 B 参考资料 257
附录 C 打印每个用户的 umask 值的脚本文件 259
附录 D 不同 UNIX 系统的命令列表 260