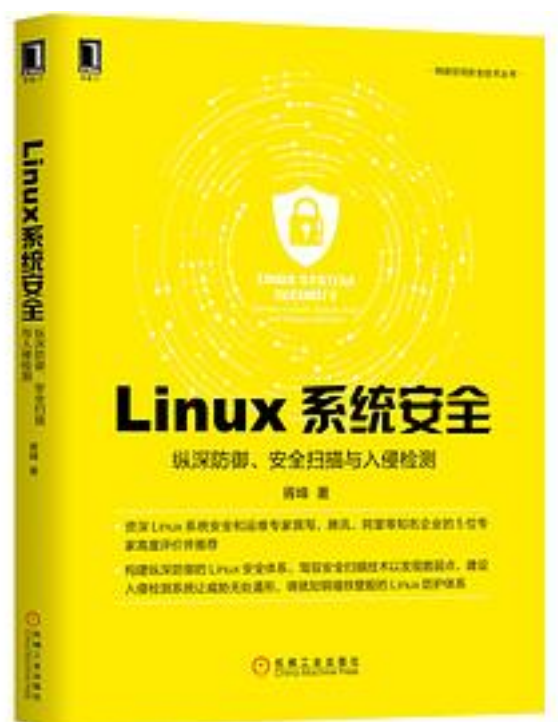


# Linux系统安全：纵深防御、安全扫描与入侵检测



[Linux系统安全：纵深防御、安全扫描与入侵检测 下载链接1](#)

著者:胥峰 著

出版者:机械工业出版社

出版时间:2019-7-20

装帧:平装

isbn:9787111632184

这是一部从技术原理、工程实践两个方面系统、深入讲解Linux系统安全的著作，从纵深防御、安全扫描、入侵检测3个维度细致讲解了如何构建一个铜墙铁壁的Linux防护体系。

作者是资深的Linux系统安全专家、运维技术专家，在该领域有13年的从业经验，厚积薄发。本书得到了来自腾讯、阿里等知名企业的多位行业专家的高度评价。全书不仅包含大量工程实践案例，而且对各种核心知识点绘制了方便记忆的思维导图。

全书共14章：

第1章介绍了安全的概念和保障安全的主要原则，引申出了“纵深防御”理念；

第2-3章是纵深防御的第一个关键步骤，即从网络层面对Linux系统进行防护，包含Linux网络防火墙和虚拟专用网络的各个方面；

第4章介绍tcpdump、RawCap、Wiresharklibpcap等网络流量分析工具的技术原理，以及用它们来定位网络安全问题的方法；

第5-7章是纵深防御的第二个关键步骤，即从操作系统层面对Linux系统进行防护，包含用户管理、软件包管理、文件系统管理等核心主题；

第8章是纵深防御的第三个关键步骤，即保障Linux应用的安全，避免应用成为黑客入侵的入口，涵盖网站安全架构、Apache安全、Nginx安全、PHP安全、Tomcat安全、Memcached安全、Redis安全、MySQL安全等话题；

第9章是纵深防御的第四个关键步骤，即确保业务连续性，防御数据被篡改或者数据丢失的风险，讲解了各种场景下的数据备份与恢复；

第10章介绍了nmap、masscan等扫描工具的原理与使用，以及各种开源和商业Web漏洞扫描工具的原理和使用；

第11-13章重点讲解了Linux系统的入侵检测，涉及Linux Rootkit、病毒木马查杀、日志与审计等主题；

第14章介绍利用威胁情报追踪最新攻击趋势、确定攻击事件性质的方法。

作者介绍:

胥峰

资深运维专家、Linux系统专家和安全技术专家，有13年Linux系统运维和安全经验，在业界颇具威望和影响力。曾就职于盛大游戏，担任架构师，参与多个重大项目的运维和保障，主导运维自动化平台的设计与实施。对DevOps、AIOps等新技术和新思想也有很深的理解。

著有畅销书《Linux运维最佳实践》，同时还翻译了DevOps领域的划时代著作《DevOps：软件架构师行动指南》。

目录: 前言

第1章 Linux系统安全概述1

1.1 什么是安全2

1.1.1 什么是信息安全2

1.1.2 信息安全的木桶原理4

1.1.3 Linux系统安全与信息安全的关系5

1.2 威胁分析模型5

1.2.1 STRIDE模型5

1.2.2 常见的安全威胁来源6

1.3 安全的原则8

1.3.1 纵深防御8

1.3.2 运用PDCA模型9

1.3.3 最小权限法则11

1.3.4 白名单机制12

|                              |    |
|------------------------------|----|
| 1.3.5 安全地失败                  | 12 |
| 1.3.6 避免通过隐藏来实现安全            | 13 |
| 1.3.7 入侵检测                   | 14 |
| 1.3.8 不要信任基础设施               | 14 |
| 1.3.9 不要信任服务                 | 15 |
| 1.3.10 交付时保持默认是安全的           | 15 |
| 1.4 组织和管理的因素                 | 16 |
| 1.4.1 加强安全意识培训               | 16 |
| 1.4.2 特别注意弱密码问题              | 17 |
| 1.4.3 明令禁止使用破解版软件            | 18 |
| 1.4.4 组建合理的安全组织结构            | 18 |
| 1.5 本章小结                     | 19 |
| 第2章 Linux网络防火墙               | 21 |
| 2.1 网络防火墙概述                  | 21 |
| 2.2 利用iptables构建网络防火墙        | 23 |
| 2.2.1 理解iptables表和链          | 23 |
| 2.2.2 实际生产中的iptables脚本编写     | 25 |
| 2.2.3 使用iptables进行网络地址转换     | 27 |
| 2.2.4 禁用iptables的连接追踪        | 29 |
| 2.3 利用Cisco防火墙设置访问控制         | 34 |
| 2.4 利用TCP Wrappers构建应用访问控制列表 | 35 |
| 2.5 利用DenyHosts防止暴力破解        | 36 |
| 2.6 在公有云上实施网络安全防护            | 38 |
| 2.6.1 减少公网暴露的云服务器数量          | 39 |
| 2.6.2 使用网络安全组防护              | 40 |
| 2.7 使用堡垒机增加系统访问的安全性          | 41 |
| 2.7.1 开源堡垒机简介                | 43 |
| 2.7.2 商业堡垒机简介                | 44 |
| 2.8 分布式拒绝服务攻击的防护措施           | 46 |
| 2.8.1 直接式分布式拒绝服务攻击           | 46 |
| 2.8.2 反射式分布式拒绝服务攻击           | 47 |
| 2.8.3 防御的思路                  | 48 |
| 2.9 局域网中ARP欺骗的防御             | 48 |
| 2.10 本章小结                    | 50 |
| 第3章 虚拟专用网络                   | 52 |
| 3.1 常见虚拟专用网络构建技术             | 53 |
| 3.1.1 PPTP虚拟专用网络的原理          | 53 |
| 3.1.2 IPSec虚拟专用网络的原理         | 53 |
| 3.1.3 SSL/TLS虚拟专用网络的原理       | 54 |
| 3.2 深入理解OpenVPN的特性           | 55 |
| 3.3 使用OpenVPN创建点到点的虚拟专用网络    | 55 |
| 3.4 使用OpenVPN创建远程访问的虚拟专用网络   | 61 |
| 3.5 使用OpenVPN创建站点到站点虚拟专用网络   | 69 |
| 3.6 回收OpenVPN客户端的证书          | 70 |
| 3.7 使用OpenVPN提供的各种script功能   | 71 |
| 3.8 OpenVPN的排错步骤             | 73 |
| 3.9 本章小结                     | 77 |
| 第4章 网络流量分析工具                 | 79 |
| 4.1 理解tcpdump工作原理            | 80 |
| 4.1.1 tcpdump的实现机制           | 80 |
| 4.1.2 tcpdump与iptables的关系    | 82 |
| 4.1.3 tcpdump的简要安装步骤         | 82 |
| 4.1.4 学习tcpdump的5个参数和过滤器     | 83 |
| 4.1.5 学习tcpdump的过滤器          | 83 |

|                           |     |
|---------------------------|-----|
| 4.2 使用RawCap抓取回环端口的数据     | 84  |
| 4.3 熟悉Wireshark的最佳配置项     | 85  |
| 4.3.1 Wireshark安装过程的注意事项  | 85  |
| 4.3.2 Wireshark的关键配置项     | 86  |
| 4.3.3 使用追踪数据流功能           | 89  |
| 4.4 使用libpcap进行自动化分析      | 90  |
| 4.5 案例1：定位非正常发包问题         | 91  |
| 4.6 案例2：分析运营商劫持问题         | 94  |
| 4.6.1 中小运营商的网络现状          | 94  |
| 4.6.2 基于下载文件的缓存劫持         | 95  |
| 4.6.3 基于页面的iframe广告嵌入劫持   | 99  |
| 4.6.4 基于伪造DNS响应的劫持        | 100 |
| 4.6.5 网卡混杂模式与raw socket技术 | 100 |
| 4.7 本章小结                  | 103 |
| 第5章 Linux用户管理             | 105 |
| 5.1 Linux用户管理的重要性         | 105 |
| 5.2 Linux用户管理的基本操作        | 107 |
| 5.2.1 增加用户                | 108 |
| 5.2.2 为用户设置密码             | 108 |
| 5.2.3 删除用户                | 109 |
| 5.2.4 修改用户属性              | 109 |
| 5.3 存储Linux用户信息的关键文件详解    | 110 |
| 5.3.1 passwd文件说明          | 110 |
| 5.3.2 shadow文件说明          | 111 |
| 5.4 Linux用户密码管理           | 112 |
| 5.4.1 密码复杂度设置             | 112 |
| 5.4.2 生成复杂密码的方法           | 113 |
| 5.4.3 弱密码检查方法             | 116 |
| 5.5 用户特权管理                | 118 |
| 5.5.1 限定可以使用su的用户         | 118 |
| 5.5.2 安全地配置sudo           | 118 |
| 5.6 关键环境变量和日志管理           | 119 |
| 5.6.1 关键环境变量设置只读          | 119 |
| 5.6.2 记录日志执行时间戳           | 119 |
| 5.7 本章小结                  | 120 |
| 第6章 Linux软件包管理            | 122 |
| 6.1 RPM概述                 | 122 |
| 6.2 使用RPM安装和移除软件          | 123 |
| 6.2.1 使用RPM安装和升级软件        | 123 |
| 6.2.2 使用RPM移除软件           | 124 |
| 6.3 获取软件包的信息              | 125 |
| 6.3.1 列出系统中已安装的所有RPM包     | 125 |
| 6.3.2 软件包的详细信息查询          | 125 |
| 6.3.3 查询哪个软件包含有指定文件       | 126 |
| 6.3.4 列出软件包中的所有文件         | 126 |
| 6.3.5 列出软件包中的配置文件         | 127 |
| 6.3.6 解压软件包内容             | 127 |
| 6.3.7 检查文件完整性             | 127 |
| 6.4 Yum及Yum源的安全管理         | 129 |
| 6.4.1 Yum简介               | 129 |
| 6.4.2 Yum源的安全管理           | 130 |
| 6.5 自启动服务管理               | 130 |
| 6.6 本章小结                  | 131 |
| 第7章 Linux文件系统管理           | 133 |

|                             |     |
|-----------------------------|-----|
| 7.1 Linux文件系统概述             | 133 |
| 7.1.1 Inode                 | 134 |
| 7.1.2 文件的权限                 | 135 |
| 7.2 SUID和SGID可执行文件          | 136 |
| 7.2.1 SUID和SGID可执行文件概述      | 136 |
| 7.2.2 使用sXid监控SUID和SGID文件变化 | 137 |
| 7.3 Linux文件系统管理的常用工具        | 137 |
| 7.3.1 使用chattr对关键文件加锁       | 137 |
| 7.3.2 使用extundelete恢复已删除文件  | 138 |
| 7.3.3 使用srm和dd安全擦除敏感文件的方法   | 141 |
| 7.4 案例：使用Python编写敏感文件扫描程序   | 141 |
| 7.5 本章小结                    | 143 |
| 第8章 Linux应用安全               | 145 |
| 8.1 简化的网站架构和数据流向            | 145 |
| 8.2 主要网站漏洞解析                | 146 |
| 8.2.1 注入漏洞                  | 147 |
| 8.2.2 跨站脚本漏洞                | 148 |
| 8.2.3 信息泄露                  | 149 |
| 8.2.4 文件解析漏洞                | 150 |
| 8.3 Apache安全                | 152 |
| 8.3.1 使用HTTPS加密网站           | 153 |
| 8.3.2 使用ModSecurity加固Web    | 154 |
| 8.3.3 关注Apache漏洞情报          | 158 |
| 8.4 Nginx安全                 | 158 |
| 8.4.1 使用HTTPS加密网站           | 158 |
| 8.4.2 使用NAXSI加固Web          | 159 |
| 8.4.3 关注Nginx漏洞情报           | 160 |
| 8.5 PHP安全                   | 160 |
| 8.5.1 PHP配置的安全选项            | 160 |
| 8.5.2 PHP开发框架的安全            | 162 |
| 8.6 Tomcat安全                | 163 |
| 8.7 Memcached安全             | 165 |
| 8.8 Redis安全                 | 165 |
| 8.9 MySQL安全                 | 166 |
| 8.10 使用公有云上的WAF服务           | 167 |
| 8.11 本章小结                   | 168 |
| 第9章 Linux数据备份与恢复            | 170 |
| 9.1 数据备份和恢复中的关键指标           | 171 |
| 9.2 Linux下的定时任务             | 172 |
| 9.2.1 本地定时任务                | 172 |
| 9.2.2 分布式定时任务系统             | 174 |
| 9.3 备份存储位置的选择               | 175 |
| 9.3.1 本地备份存储                | 175 |
| 9.3.2 远程备份存储                | 176 |
| 9.3.3 离线备份                  | 177 |
| 9.4 数据备份                    | 178 |
| 9.4.1 文件备份                  | 178 |
| 9.4.2 数据库备份                 | 179 |
| 9.5 备份加密                    | 181 |
| 9.6 数据库恢复                   | 182 |
| 9.7 生产环境中的大规模备份系统案例         | 182 |
| 9.8 本章小结                    | 184 |
| 第10章 Linux安全扫描工具            | 186 |
| 10.1 需要重点关注的敏感端口列表          | 186 |

|                                           |     |
|-------------------------------------------|-----|
| 10.2 扫描工具nmap                             | 188 |
| 10.2.1 使用源码安装nmap                         | 188 |
| 10.2.2 使用nmap进行主机发现                       | 189 |
| 10.2.3 使用nmap进行TCP端口扫描                    | 190 |
| 10.2.4 使用nmap进行UDP端口扫描                    | 192 |
| 10.2.5 使用nmap识别应用                         | 192 |
| 10.3 扫描工具masscan                          | 193 |
| 10.3.1 安装masscan                          | 193 |
| 10.3.2 masscan用法示例                        | 193 |
| 10.3.3 联合使用masscan和nmap                   | 194 |
| 10.4 开源Web漏洞扫描工具                          | 195 |
| 10.4.1 Nikto                              | 195 |
| 10.4.2 OpenVAS                            | 196 |
| 10.4.3 SQLMap                             | 198 |
| 10.5 商业Web漏洞扫描工具                          | 199 |
| 10.5.1 Nessus                             | 199 |
| 10.5.2 Acunetix Web Vulnerability Scanner | 201 |
| 10.6 本章小结                                 | 202 |
| 第11章 入侵检测系统                               | 204 |
| 11.1 IDS与IPS                              | 204 |
| 11.2 开源HIDS OSSEC部署实践                     | 205 |
| 11.3 商业主机入侵检测系统                           | 214 |
| 11.3.1 青藤云                                | 215 |
| 11.3.2 安全狗                                | 215 |
| 11.3.3 安骑士                                | 215 |
| 11.4 Linux Prelink对文件完整性检查的影响             | 217 |
| 11.5 利用Kippo搭建SSH蜜罐                       | 218 |
| 11.5.1 Kippo简介                            | 218 |
| 11.5.2 Kippo安装                            | 219 |
| 11.5.3 Kippo捕获入侵案例分析                      | 220 |
| 11.6 本章小结                                 | 221 |
| 第12章 Linux Rootkit与病毒木马检查                 | 223 |
| 12.1 Rootkit分类和原理                         | 223 |
| 12.2 可加载内核模块                              | 225 |
| 12.3 利用Chkrootkit检查Rootkit                | 226 |
| 12.3.1 Chkrootkit安装                       | 227 |
| 12.3.2 执行Chkrootkit                       | 227 |
| 12.4 利用Rkhunter检查Rootkit                  | 228 |
| 12.4.1 Rkhunter安装                         | 228 |
| 12.4.2 执行Rkhunter                         | 228 |
| 12.5 利用ClamAV扫描病毒木马                       | 229 |
| 12.6 可疑文件的在线病毒木马检查                        | 230 |
| 12.6.1 VirusTotal                         | 231 |
| 12.6.2 VirSCAN                            | 231 |
| 12.6.3 Jotti                              | 232 |
| 12.7 Webshell检测                           | 232 |
| 12.7.1 D盾                                 | 233 |
| 12.7.2 LMD检查Webshell                      | 234 |
| 12.8 本章小结                                 | 235 |
| 第13章 日志与审计                                | 237 |
| 13.1 搭建远程日志收集系统                           | 237 |
| 13.1.1 Syslog-ng server搭建                 | 238 |
| 13.1.2 Rsyslog/Syslog client配置            | 239 |
| 13.2 利用Audit审计系统行为                        | 239 |

13.2.1 审计目标239  
13.2.2 组件240  
13.2.3 安装241  
13.2.4 配置241  
13.2.5 转换系统调用242  
13.2.6 审计Linux的进程243  
13.2.7 按照用户来审计文件访问244  
13.3 利用unhide审计隐藏进程244  
13.4 利用lsof审计进程打开文件245  
13.5 利用netstat审计网络连接246  
13.6 本章小结246  
第14章 威胁情报248  
14.1 威胁情报的概况248  
14.2 主流威胁情报介绍249  
14.2.1 微步在线威胁情报社区249  
14.2.2 360威胁情报中心252  
14.2.3 IBM威胁情报中心253  
14.3 利用威胁情报提高攻击检测与防御能力254  
14.4 本章小结255  
附录A 网站安全开发的原则257  
附录B Linux系统被入侵后的排查过程273  
• • • • • ([收起](#))

[Linux系统安全：纵深防御、安全扫描与入侵检测 下载链接1](#)

## 标签

安全

Linux

计算机

linux

好书，值得一读

信息安全

科技

实用

## 评论

贵行业出书的门槛也太低了吧

-----  
从网络层面、操作系统层面、应用层面和业务连续性4个方面，实现Linux系统的纵深防御。

-----  
看完目录决定入手，收到后惊喜地发现每一章还附赠一章思维导图，方便回顾和记忆，这就很贴心，哈哈~

-----  
目前生产环境中绝大部分用的都是Linux系统，它的安全性太重要了，这也是个老话题，但是这本书是第一个将这个问题阐述得如此深入、全面的。

-----  
这特么评论刷的吧，不适合新人好嘛！！  
在这个系列里，和那本数据安全架构的书，刷好评的演员怪不得这么眼熟去你妈的。

-----  
没有绝对安全的系统。没有攻不破的系统，只有还没攻破的系统。Linux系统安全是一个庞大的体系，而本书几乎涵盖了保障Linux系统安全的方方面面。这本书既有原理剖析，也有实践指导，是一本该行业从业者或是对Linux安全技术有兴趣者值得读读的书。

-----  
胥峰老师在Linux和运维领域大名鼎鼎，书如其人，一个字，牛！

-----  
适合新书入门，也适合有一定工作经验的安全从业人员阅读。纵览这本书，让人收获很多。首先它不是简单的说教，也不是长篇大论的理论分析，而是以案例为入口，贴近实战。其次，每章都有清晰的知识脑图，非常有助于读者把握各章内容的关联关系，也非



常方便读者快速记忆核心知识点。作为一个安全工程师，我推荐这本书。

-----  
要想拥有一个安全的Linux系统，感觉看这本书足够了，知识点非常全面，几乎面面俱到。

-----  
这本书，结构完整体系化，内容详实且深入浅出，非常赞的一本书。

-----  
拿到书后，如饥似渴的读了起来。内容写的很好，从安全的用户管理到软件管理、Mas scan/Nmap扫描工具的使用、开源入侵检测工具OSSEC的部署安全，非常详尽。希望这本书助我早日成为Linux安全大牛。

-----  
胥峰大神的新书，是一定要来支持一下的，他的个人品牌就是内容质量的保证。

-----  
难得有书能系统详细的介绍Linux系统安全，填补了这项空白。

-----  
[Linux系统安全：纵深防御、安全扫描与入侵检测\\_下载链接1\\_](#)

## 书评

-----  
[Linux系统安全：纵深防御、安全扫描与入侵检测\\_下载链接1\\_](#)