6 linux系统安全

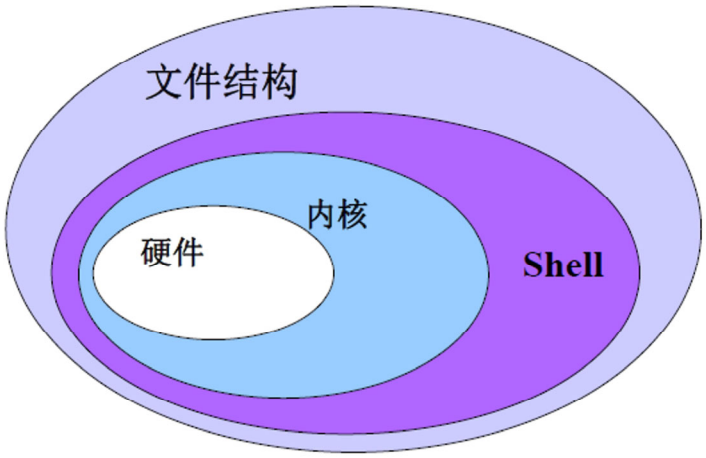
2019年4月10日 23:36

1 Linux安全概述

1.1 Linux操作系统简介

Linux的组成

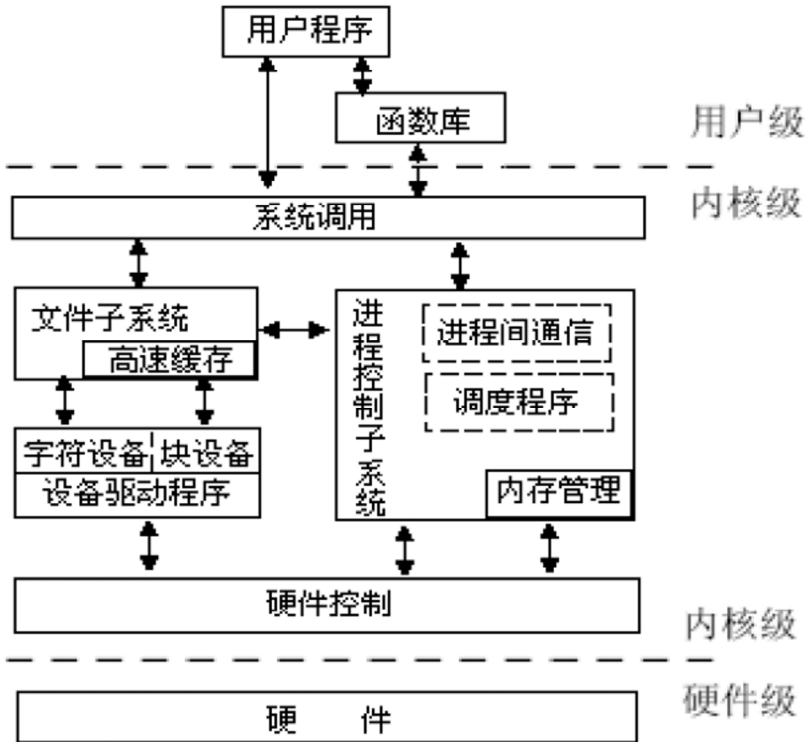
- 内核
- 硬件
- 文件结构
- 实用工具

- 

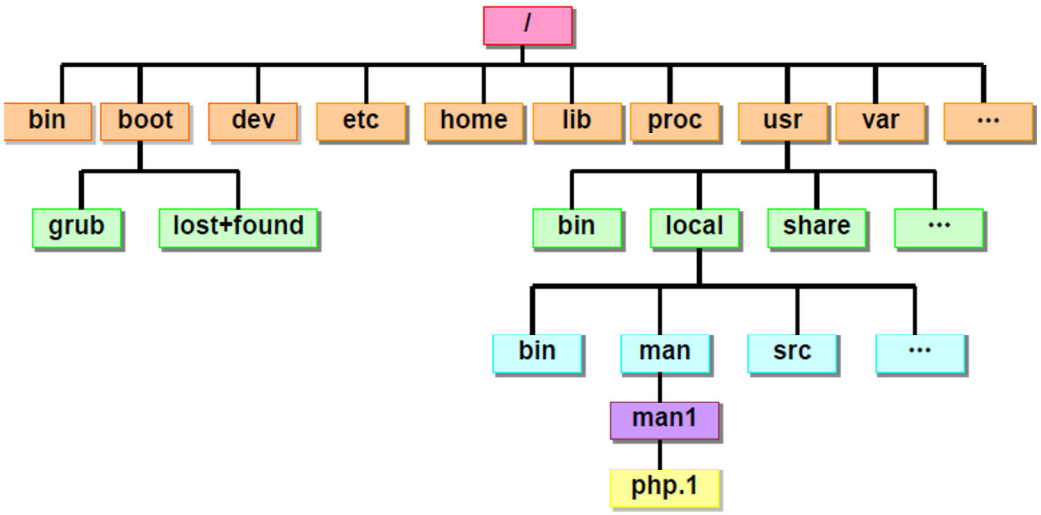
Linux内核的子系统组成

- 进程控制（进程调度，进程间通信）
- 内存管理
- 虚拟文件系统
- 网络接口（网络协议，网络设备驱动）

Linux内核的结构

- 

Linux目录结构及目录路径

- 

目录介绍

-

目录名	说明
/	Linux系统根目录
/bin	存放普通用户可执行文件，系统中的任何用户都可以执行该目录中的命令
/sbin	存放系统的管理命令，普通用户不能执行该目录中的命令
/home	普通用户的主目录，每个用户在该目录下都有一个与用户名同时的目录
/etc	存放系统配置和管理文件，这些文件都是文本文件
/boot	存放内核和系统启动程序
/usr	该目录最庞大，存放应用程序及相关文件
/dev	存放设备文件
/proc	虚拟的目录，是系统内存的映射。可直接访问这个目录来获取系统信息。
/var	用于存放大系统中经常变化的文件，如日志文件，用户邮件邮件等
/tmp	公用的临时文件存储点

Linux系统的启动过程

1. BIOS加电自检
2. 加载主引导记录MBR
3. 加载操作系统装载器
4. 加载Linux内核映像
5. 加载init进程
6. 接受用户登录

Linux操作系统的引导过程

Linux内核获得控制权后，将会按以下步骤继续引导系统。

1. 首先检测系统中的硬件设备，对其进行初始化。
2. 它要对自身进行解压，并加载必要的设备驱动。
3. 初始化与文件系统相关的虚拟设备。
4. 装载根文件系统（/），把其挂载到根目录下。
5. 加载init程序，并把控制权交给init进程，由其继续完成接下来的系统引导工作。

Init进程

- 内核映像在完成引导后，便会启动init进程，init进程对应的执行文为/sbin/init。
- Linux系统中的所有进程都由init进程衍生，其进程号是1。
- 如果init进程出现问题，系统中的其他进程也会随之而受影响。

init进程的引导过程

当init进程获得控制权后，会首先执行/etc/rcd/rcsysinit脚本。

- 配置环境变量
- 配置网络
- 启用Swap
- 检查并挂载文件系统
- 执行其他必须的系统初始化步骤。

1.2 Linux系统的安全威胁

- 特权程序漏洞
- 恶意代码
- 网络监听和数据捕获
- 软件设置和相互作用

1.3 Linux系统的安全机制

- 标识（UID和GID）
- 鉴别
- 访问控制
- 审计
- 网络安全防护（防火墙、入侵检测、完整性保护、安全传输）

2 Linux本地安全机制

2.1 用户和组安全

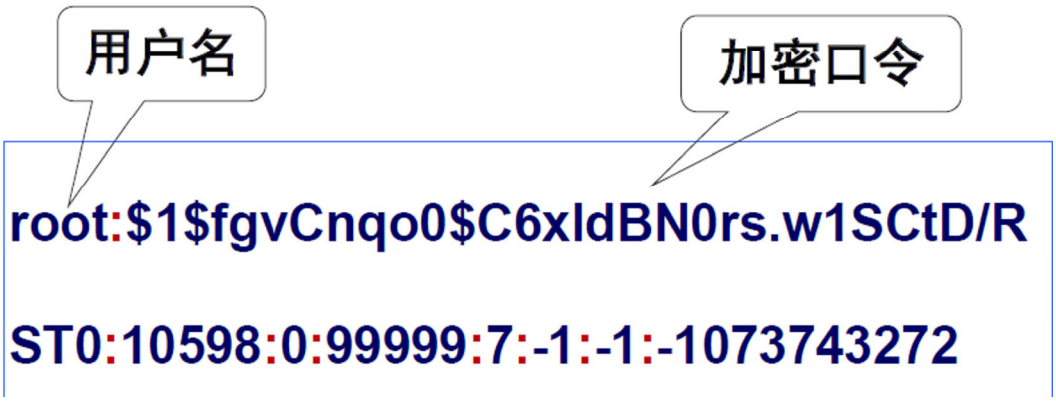
- Linux系统中文件和程序的访问控制以用户(UID)和用户分组（GID）为基础
- 保护用户和组管理安全非常重要

Linux用户类型

- 根用户(root):系统的超级用户，拥有系统的最高权限。
- 普通用户:由系统管理员手创建的，可以登录系统，但只能操作自己拥有权限的文件

用户和组文件

- 用户配置文件/etc/passwd
  - 所有用户可读
  - 

- 用户影子文件/etc/shadow
  - 只有root可读
  - 

- 系统组账号配置文件/etc/group
  - 用户组信息，对访问控制非必要
    - 用户分组名；
    - 加密的用户分组口令；
    - 用户分组ID号
    - 成员用户清单
  - 组口令安全存储/etc/gshadow

用户和组安全措施

- 注释掉不需要的用户和组
- 将重要文件设为不可修改
  - /etc/passwd、/etc/shadow、
  - /etc/group、/etc/gshaodw
- 编辑/etc/logindefs，设置口令复杂度策略

- 口令长度
- 生存期
- 过期告警策略

2.2 文件系统安全

- Linux系统核心支持多种文件系统类型
- Ext:Extendedfilesystem，扩展文件系统

  Ext/Ext2/Ext3/Ext4

(了解)Linux系统基本的文件类型

- 普通文件：文本文件和二进制文件
- 目录文件：存储一组文件的位置、大小等信息
- 设备文件：块设备文件和字符设备文件
- 链接文件：指向一个真实存在的文件的链接
- 管道文件：用于进程间的信息传递

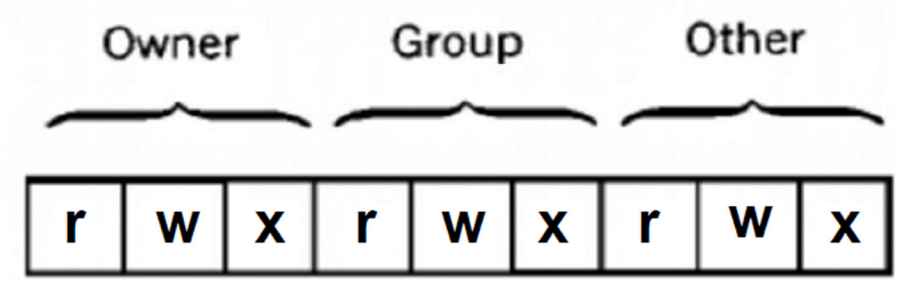
Linux文件和目录的访问权限

- 每个文件或目录都有自己的访问权限，决定谁能访问、如何访问它们。
- 权限有3种：r、w和x，对文件和目录其含义不尽相同。
-

权限	文件	目录
r	可以查看文件的内容	可以列出目录中的内容
w	可以更改文件的内容	可以在目录中添加、删除文件
x	可以执行文件，需要同时具有r权限。	可以进入目录，例如使用cd命令。

Linux文件和目录支持Owner/Group/Other访问控制机制

-



- Owner：客体属主的访问权限
- Group：与Owner同组的用户对该客体的访问权限
- Other：余下的其他用户对该客体的访问权限

说明

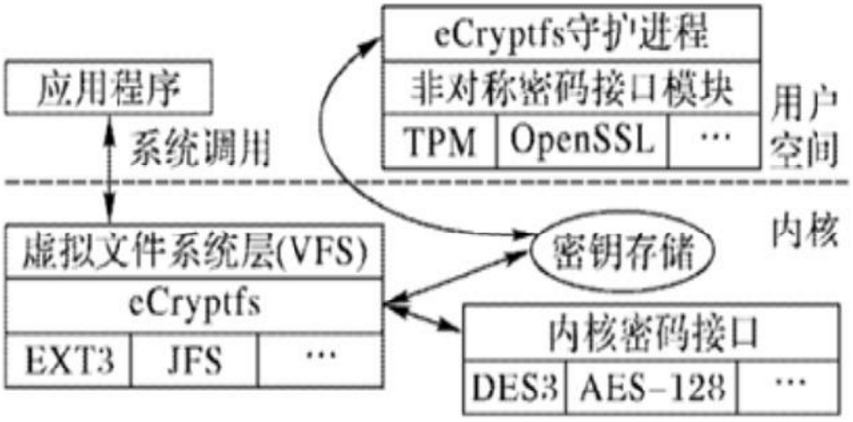
-
```
zemao@zemao-ThinkPad-R61 ~ $ ls -l
total 228060
drwxr-xr-x  9 zemao zemao      4096 2014-06-12 18:56 as3-file-transfer-read-only
drwxr-xr-x  3 zemao zemao      4096 2014-06-21 16:16 Desktop
drwxr-xr-x 33 zemao zemao     36864 2014-06-21 13:30 Downloads
-rw-r--r--  1 zemao zemao    164864 2012-06-27 14:38 dsp程序保护.doc
drwxr-xr-x  5 zemao zemao      4096 2001-09-26 22:21 EnglishAudios
-rw-r--r--  1 zemao zemao   3379712 2014-04-27 08:19 Flex开发技巧.doc
-rw-r--r--  1 zemao zemao     68096 2014-04-27 11:30 Flex教程.doc
```
- 10个标志位
  - 第1个：d(目录),b(块系统设备),c(字符设备),(普通文件)
  - 第2-4个：所有者的读、写、执行权限
  - 第5-7个标志：所有者所在组的读、写、执行权限
  - 第8-10个标志：其他用户的读、写、执行权限
- 文件所有者
  - 文件所有者的id
  - 文件所有者所在组的id

提高文件系统权限管理的灵活性

- Owner/Group/Other方式的自主访问控制不灵活
- POSIX ACLs for Linux软件包
  - 用ACL来管理权限
  - 下载并安装补丁：http://acl.bestbits.at
  - 重新编译内核
  - 两个命令：setfacl、getfacl

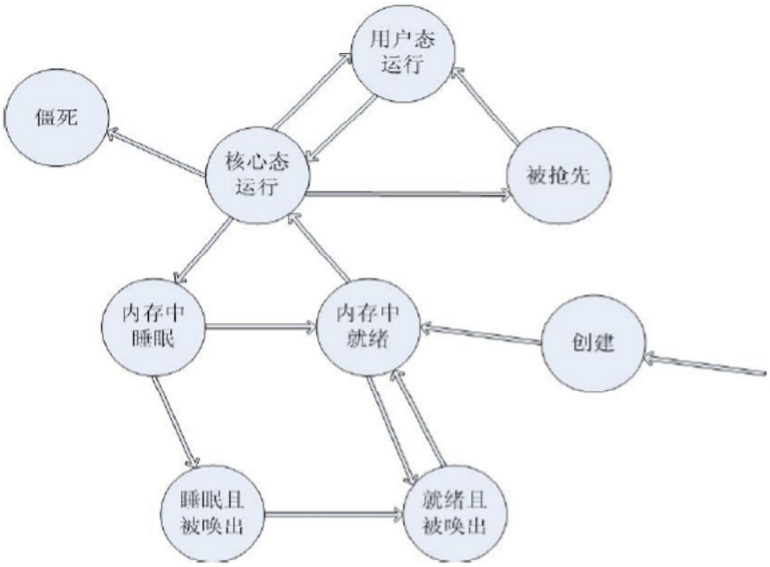
(补充自学)加密文件系统

eCryptfs加密文件系统的架构

- 

2.3 进程管理安全

- Linux系统中的进程状态

- 

- 僵尸进程
  - 一个进程调用了exit后，并非马上消失，而是留下一个称为僵尸进程（Zombie）的数据结构。
  - 僵尸进程放弃了几乎所有内存空间，无任何可执行代码，也不能被调度，仅仅在进程表中保留一个位置，记载该进程的退出状态等信息供其他进程收集。
  - 僵尸进程问题
    - Linux系统中进程数目是有限制的；
    - 如果存在太多的僵尸进程，会占用内存资源，影响系统性能和新进程的产生，甚至导致系统瘫痪。

(不考)2.4 日志管理

主要功能：审计和监测

- 连接时间日志
- 进程日志
- 错误日志
- 实用程序日志

用户登录日志

- /var/log/btmp
  - 保存用户登录失败的日志记录，用lastb命令查看。
- /var/log/wtmp
  - 保存用户成功登录的日志记录，用last命令查看。

Syslog机制

- Unix和Linux操作系统多采用syslog进行系统日志的管理和配置。
- syslog可以根据信息的来源、信息的重要程度，将信息保存到不同的日志文件
- 在默认的syslog配置下，日志文件通常都保存在“/var/log”目录下。

Syslog的组成

- 守护进程/etc/syslogd
  - 接收访问系统的日志信息，根据配置文件处理接收到的信息；希望生成日志的程序通过向syslog接口呼叫，生成日志信息。
- 配置文件/etc/syslogconf

Syslog的配置与测试

- syslog的配置文件为/etc/syslogconf，该文件指定：
  - 要记录哪些日志消息
  - 将日志消息记录到哪个日志文件
  - 日志文件的保存位置
    本地日志
    远程日志
- 用logger命令模拟产生各类的syslog消息，以测试syslog配置是否正确。
- 比syslog更强大的日志系统——Rsyslog

(不考)3 Linux网络安全技术

3.1 Web服务安全

- 配置特定的用户运行Apache服务器
  - 一般情况下，启动Apache服务器进程httpd需要root权限，存在风险
  - 安全措施：修改httpd主配置文件httpconf
    - Userapache
    - Groupapache
  - 采用root身份运行httpd后，该进程的用户和用户组权限改为apache
- 配置隐藏Apache服务器的版本号
  - 修改Apache服务器httpd主配置文件httpconf
    - SeverTokens:不向客户端输出服务器系统类型等信息
    - SeverSignture：默认为off，不输出任何系统生成的页面。
- 访问控制
  - order指令：指定执行允许访问控制规则或者禁止访问控制规则的顺序
    - allow,deny
    - deny,allow
  - allow指令：指定允许访问的地址或地址序列

        - allow from all
    - deny指令：指定禁止访问的地址或地址序列
        - deny from all
- 认证和授权保护
    - httpd主配置文件httpconf的Directory容器中
        - AuthName:定义受保护区域的名称
        - AuthType：指定使用的认证方式
        - AuthGroupFile:指定认证组文件的位置
        - AuthUserFile：指定认证口令文件的位置
    - 口令文件应放在不能被网络访问的位置
- 设置虚拟目录
    - 创建虚拟目录，从主目录以外的其他目录进行发布；
    - 虚拟目录设置不同的访问权限；
    - 虚拟目录只有特定用户知道。
- Apache服务器的安全模块-提供Apache的访问控制、认证、授权等安全服务
    - mod_access:基于主机的访问控制
    - mod_auth:控制用户和组的认证授权
    - mod_auth_db和mod_auth_db模块:
    - mod_auth_digest模块:
    - mod_auth_anon模块:
    - mod_ssl模块:
- 应用SSL技术
    - 使用SSL技术对网络传输数据进行加密。
    - 通过获得证书，保证客户连接的服务器没有被仿冒。

3.2 Netfilter/Iptables防火墙

Netfilter工作在内核，Iptables允许用户定义访问控制规则。

- 包过滤
- NAT
- 数据包处理

3.3 入侵检测

Snort

- 轻量级的网络入侵检测(NetworkIntrusionDetectionSystem)，即NIDS
- 三种工作模式
    - 嗅探器
    - 数据包记录器
    - 网络入侵检测系统

3.4 DNS服务安全

- BerkeleyBIND软件
- 安全措施
    - 配置辅助域名服务器
    - 配置高速缓存服务器
    - 负载均衡
    - 配置DNS查询方式
    - DNSSEC安全防护：来源验证、完整性验证和否定存在验证

3.5 DHCP服务安全

- 系统自带的rpm包
- dhcpd软件
- chroot机制
    - 将DHCP软件运行限制在指定目录中
    - chroot“牢笼”

3.6 xinetd

网络服务管理程序

- 存取控制
- Dos攻击防御
- 日志功能
- 请求转发
- IPv6
- 与客户端交互