**linux基本防护**

用户账户安全

设置帐号有效期

使用chage工具

-d 0,强制修改密码

-E yyyy-mm-dd，指定失效日期（-l取消）

帐号的锁定/解锁

使用passwd命令

-l锁定、-u解锁、-S查看状态

强制定期修改密码

配置文件/etc/login.defs（对新建的用户有效）

主要控制属性

PASS\_MAX\_DAYS

PASS\_MIN\_DAYS

PASS\_WARN\_AGE

伪登录提示

配置文件/etc/issue、/etc/issue.net

分别适用于本地、远程登录

默认会提示内核、系统等版本信息

文件系统安全

程序和服务控制

禁用非必要的系统服务（使用systemctl、chkconfig工具）

锁定/解锁保护文件

EXT3/EXT4的文件属性控制

chattr、lsattr

+ - =控制方式

属性i：不可变

属性a：仅可追加

**用户切换与提权**

su切换用户身份

切换与提权的应用场景

切换身份，when

SSH远程管理

运维测试

提升执行权限，when

管理权限细分

su切换的基本用法

快速切换为指定的其他用户

普通用户执行时，需验证目标用户的密码

root执行时，无需验证口令

命令格式

用法1：su [-] [目标用户]

用法2：su [-] -c “命令” [目标用户]

sudo提升执行权限

sudo提权的基本用法（超级执行）

管理员预先为用户设置执行许可

被授权用户有权执行授权的命令，验证自己的口令

命令格式

用法1：sudo 特权命令

用法2：sudo [-u 目标用户] 特权命令

配置sudo授权

修改方法

推荐：visudo

其他：vim /etc/sudoers

授权记录格式

用户 主机列表=命令列表



sudo别名设置

主要用途

提高可重用性、易读性

简化配置、使记录更有条理



**SSH访问控制**

SSH基本防护

SSH防护概述

存在的安全隐患

密码嗅探、键盘记录

暴力枚举帐号、猜解密码

常见的防护措施

用户限制、黑白名单

更改验证方式（密码->密钥对）

防火墙

sshd基本安全配置

配置文件/etc/ssh/sshd\_config

port 3389 //改用非标准端口

protocol 2 //启用SSH V2版协议

listenaddress 192.168.168.174

permitrootlogin no //禁止root登录

usedns no //不解析客户机地址

logingracetime 1m //登录限时

maxauthtries 3 //每连接最多认证次数

sshd黑/白名单配置

配置文件/etc/ssh/sshd\_config

DenyUsers user1 user2

AllowUsers user1@host user2

DenyGroups group1 group2

AllowGroups group1 group2

SSH密钥对验证

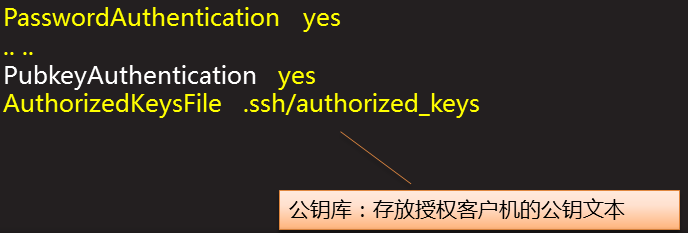
sshd验证方式登录

口令验证

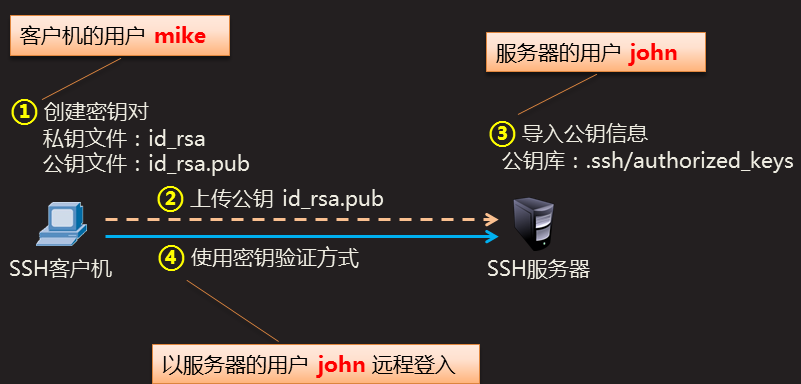
检查登录用户的口令是否一致

密钥验证

检查客户端私钥与服务器上的公钥是否匹配



密钥对验证的实现思路



创建密钥对

使用工具ssh-keygen

可以手动指定加密算法（-t rsa 或 -t dsa）

若不指定，默认采用RSA加密

部署公钥

方法一，通过ssh-copy-id自动部署

好处：一步到位

局限性：要求SSH口令认证可用

方法二，通过FTP等方式上传、手动添加

好处：灵活，适用范围广

局限性：操作繁琐、易出错

测试SSH密钥对验证

客户端登录操作

仅限密钥对创建人适用

需要验证私钥口令（如果有的话，否则免密登录）

**selinux安全防护**

selinux概述

什么是Selinux

一套强化linux安全的扩展模块

美国国家安全局主导研发

selinux的运作机制

集成到linux内核（2.6及以上）

操作系统提供可定制的策略、管理工具

红帽的selinux策略集

selinuxtype=targeted

推荐，仅保护最常见/关键的网络服务，其他不限制

主要软件包：

selinux-policy、selinux-policy-targeted、libselinux-utils、libselinux-utils、coreutils、policycoreutils

selinux模式控制

方法一，修改kernel启动参数

添加selinux=0以禁用

添加enforce=0设置selinux为允许模式

方法二：修改文件/etc/selinux/config

设置selinux=disabled以禁用

设置selinux=permissive宽松/允许模式

设置selinux=enforceing强制模式

selinux开关控制

临时调整，setenforce命令（非disabled状态下才可用）

设置为1，对应强制模式

设置为0，对应宽松模式

selinux策略设置

查看安全上下文

安全上下文：为文本/目录/设备标记访问控制属性

属性构成：用户:角色:访问类型:选项...

常见的访问类型：

|  |  |
| --- | --- |
| 类型 | 用途 |
| bin\_t | 二进制执行文件 |
| etc\_t | 系统配置文件 |
| fsadm\_exec\_t | 文件系统管理 |
| admin\_home\_t | 管理员账户的宿主目录 |
| user\_home\_t | 普通用户的宿主目录 |
| httpd\_sys\_content\_t | http网站内容 |

修改安全上下文

使用chcon工具

-t，指定访问类型

-R，递归修改

一般操作规律

移动的文件，原有的上下文属性不变

复制的文件，自动继承目标位置的上下文

重置安全上下文

使用restorecon工具

恢复为所在位置的默认上下文属性

-R，递归修改

/.autorelabel文件

下次重启后全部重置

调整Selinux布尔值

使用getsebool查看

-a，可列出所有布尔值

使用setsebool设置

-P，永久更改，重启后仍然有效