



信息安全综合实践

课程简介

网络空间安全学院 刘铭



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

课程简介

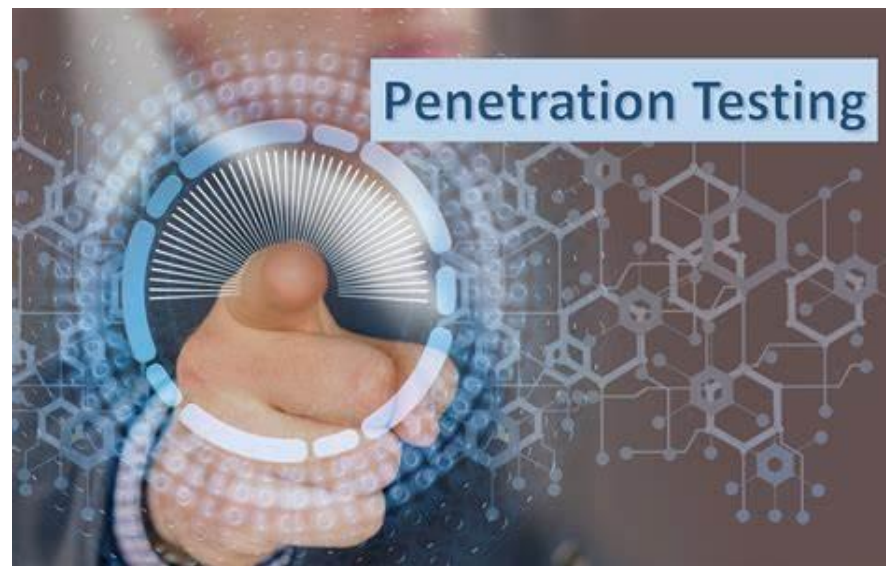


本课程是信息安全专业的**实验实践课程**。学习信息安全理论和实验实践方法。掌握实际应用环境中进行信息安全攻防的技术方法。

1. 系统安全
2. 密码技术应用（两部分）
3. 网络安全漏洞
4. 渗透测试（两部分）

课程组成

1. 课堂讲座，本教室。
2. 实验课，电信群楼4-406实验室。
3. 学生报告会，本教室。



课程内容



讲座课

- 第1、3、5、7、9、11周。实验所需理论知识。

实验以及实验作业

- 实验：双周（第2、4、6、8、10、12、14、16周）每周二的第6-8节课。地点在电信群楼4-406。第一次实验课安排在**9月19号**，系统安全实验。
- 实验作业：共六次实验作业。实验作业完成时间为两周左右。最后两周无实验作业。

报告会

- 第13、15周。请每位同学准备10分钟的PPT报告（Pre），内容为信息安全实践技术分享。选题鼓励深入探索，需要有具体的实验过程。可以是实验课内容的进一步延伸。

课程安排



周次	讲座、报告会	实验	考核方式
1	系统安全		参与
2		系统安全实验	实验作业
3	密码技术概述		参与
4		密码技术实验（1） OpenSSL, PGP	实验作业
5	密码技术应用		参与
6		密码技术实验（2） OpenSSH	实验作业
7	漏洞利用		参与
8		漏洞实验，SQL注入实验	实验作业
9	渗透测试（1）		参与
10		渗透测试实验（1）	实验作业
11	渗透测试（2）		参与
12		渗透测试实验（2）	实验作业
13	学生报告会（1） 课堂报告（10分钟/人）		参与
14		信息安全综合实验（1）	无作业
15	学生报告会（2） 课堂报告（10分钟/人）		参与
16		信息安全综合实验（2）	无作业

考核方式



考核方式	实验作业（70分）	平时成绩（30分）
具体内容	<ul style="list-style-type: none">实验作业（六次）	<ul style="list-style-type: none">讲座课/实验课/报告会参与学生报告会报告（10分钟Pre）

其他事项



1. 作业分享

- 第三、五、七、九、十一周
- 根据内容延伸情况对平时成绩进行额外加分
- 每位同学可报名一次作业分享，通过邮箱报名
- 是否报名成功会回复邮件

2. 报告会顺序

- 13、15周
- 根据本课程所学内容自行选择实验，需要有延伸
- 顺序会在第四周左右公布，公布之后尽量不要修改

3. 推荐上课/实验携带自己电脑

4. 实验签到

报告会评分标准（13、15）



- 选题（2分）信息安全技术复现，可以是实验课内容的进一步延伸。
- 实验（2分）具体的实验过程（Kali, DVWA, Burpsuite, SQLmap, Hydra, Sparta, Nmap, Setoolkit, Ettercap, Nessus, Awvs, Metasploit, Kiwi...)
- 深度（2分）技术的深入程度
- 工作量（2分）至少一次实验课的工作量
- 展示质量（2分）10分钟展示

特别提示



1. 本课程提供的程序和方法可能带有攻击性，仅供安全研究与教学使用。
2. 在课程中，任何测试仅在虚拟机内运行，不对公网的任何设施进行安全检测和攻击。
3. 作业不得照抄其他同学的内容。（实验截图）
4. Pre需要有具体的实验过程。



信息安全综合实践

系统安全



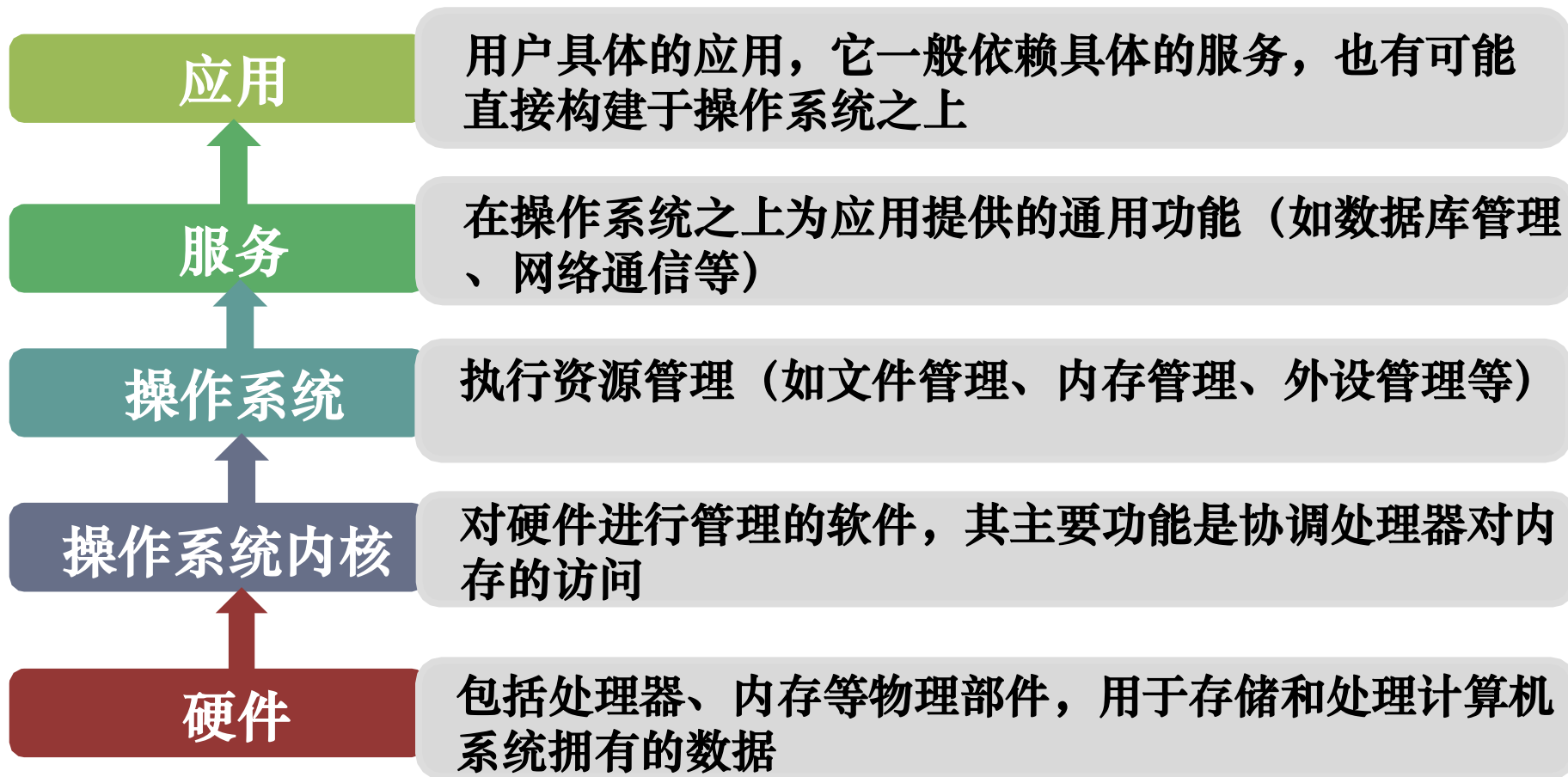
上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

本节内容

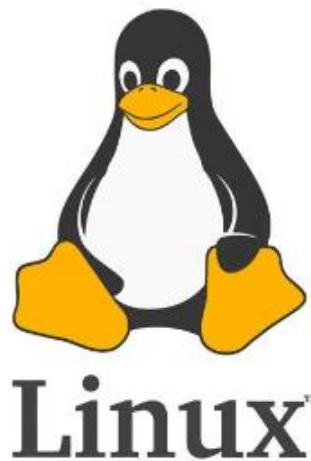


- **操作系统的功能**
- **操作系统安全**
- **操作系统安全模型**

计算机系统的层次结构



常见的操作系统

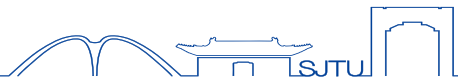


可以从安全操作系统**本身**和操作系统安全**加固**两个方面来考虑

- **安全操作系统**：试图设计和开发一个安全的操作系统本身
- **操作系统安全加固**：对已有的操作系统进行安全性设置和配置

构建安全操作系统需要大量的研发工作和资源，而且可能不适用于所有用例

操作系统安全的发展



1969 年，第一个
分时安全操作系统
Adept-50出现

Lampson提出**访问
控制**(access
control)的概念

1970 年，W.H.
Ware提出**多级安
全**multi-level
security system

1972年，J.P.
Anderson提出
必须建立系统的
安全模型，再进
行**安全内核**的设
计与实现。

1975 年，
Saltzer 和
Schroeder
提出了安全
操作系统
的设计**原则**

1985 年，颁
布了历史上第
一个计算机安
全评价标准
TCSEC

操作系统安全的原则



- 最小特权原则：对于系统中的每个用户和程序，必须按照“**需要**”原则，给予**尽可能少的使用权限**。限制潜在的操作错误和恶意攻击。
- 可用性原则：安全性不应该以牺牲系统的可用性为代价。系统应该在合理的时间内对合法用户提供所需的服务。
- 开放性原则：保护机制应该是**公开**的，系统的安全性不应依赖于系统设计的保密性，而是要通过健全的安全机制来实现。
- 完整的**访问控制**机制：操作系统对每个访问，都必须进行合法性检查。

反面例子



违反了“最小特权原则”的反面例子：

- 某公司内部使用了一个**文件共享服务器**（例如NFS和Samba服务），用于存储内部文档。为了方便员工的访问，系统管理员为所有员工的用户账户提供了**管理员级别的访问权限**，这包括读取、写入和删除文件的权限。
- 这种情况下，员工可以**无意中删除或修改重要文件**，获取不应该访问的**敏感数据**。

建议：

1. 仅授予员工访问他们需要的特定文件或文件夹的权限，而不是为他们提供过多的权限。使用**细粒度的访问控制**来确保每个员工只能访问与其工作任务相关的文件。
2. **定期审查和更新权限**，以确保员工的权限与其职责保持一致。
3. 实施**审计和监控机制**，以检测和报告不正常的文件访问活动。

练习



哪一项原则强调了在设计系统安全性时，应该确保系统的设计不依赖于保密性，而是要通过健全的安全机制来实现？

A 最小特权原则

B 可用性原则

C 开放性原则

D 完整的访问控制机制

练习



哪一项原则强调了在设计系统安全性时，应该确保系统的设计不依赖于保密性，而是要通过健全的安全机制来实现？

A 最小特权原则

B 可用性原则

C 开放性原则

D 完整的访问控制机制

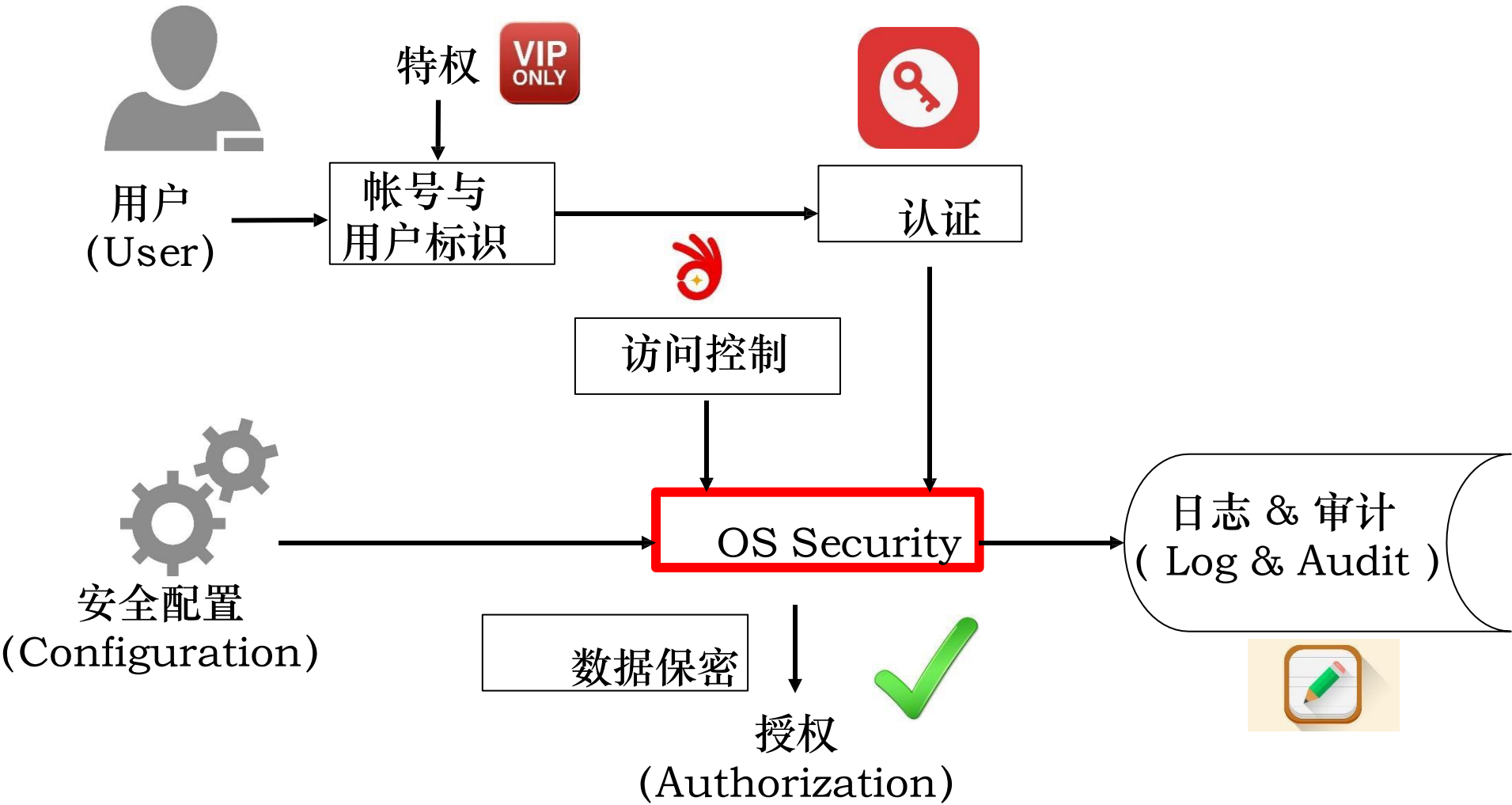
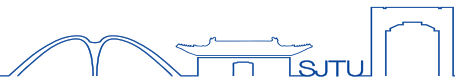
操作系统安全模型



安全模型定义**进程**对特定**资源**可以进行何种类型的访问

- 使用这个模型时，首先必须确保主体通过了**认证**；
- 当用户通过了认证后，依据**访问控制**策略给予用户访问资源的授权；
- 文件保密、文件系统**保密**；
- 操作系统也需要对用户的操作进行**日志**记录和审计。

操作系统安全模型图示



身份认证：什么是身份认证



用户或实体声称自己是特定的身份并验证。身份认证对于保护计算机系统和数据非常重要，以防止未经授权的访问、数据泄露和潜在的恶意活动。

- **身份声称(ID)**：用户或实体声称自己是特定的身份，提供标识信息（如用户名、ID等）来表明。
- **身份验证信息**：为了验证身份声称的有效性，用户或实体需要提供一些特定的身份验证信息。包括密码、生物特征（如指纹或虹膜扫描）、数字证书等。
- **身份验证过程**：将提供的身份验证信息与存储在系统中的已知信息进行比对。如果匹配成功，则身份认证成功。
- **授权和访问控制**：一旦用户或实体的身份得到验证，系统可以根据其身份授予相应的权限，以确定其能够访问的资源和执行的操作。

场景1



一个用户试图登录一个手机银行app来访问其银行账户。

- 身份声称(ID): **手机号**
- 身份验证信息: 为了验证身份声称的有效性, 系统要求用户提供**密码**, 以证明他们确实是账户的合法持有者。
- 身份验证过程: 系统将用户输入的用户名和密码与存储在系统**数据库**中的已知信息进行**比对**。如果输入的密码与数据库中的密码匹配成功, 系统将确认用户的身份认证成功。
- 授权和访问控制: 一旦用户的身份得到验证, 系统将根据其账户的权限配置, 授予用户对银行账户的访问权限。用户可以**查看账户余额**、进行**转账**等操作, 但不能执行与其授权范围之外的操作。

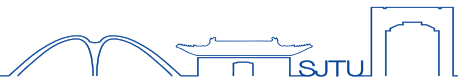
场景2



一个用户试图登录到一个运行Linux操作系统的服务器。

- 身份声称(ID): 用户声称自己是系统的合法用户，提供了一个用户名，比如 “test”。
- 身份验证信息: 用户需要验证自己的身份，通常通过输入与其账户关联的密码。
- 身份验证过程: 系统将用户提供的用户名和密码与系统中的用户数据库（/etc/passwd文件和/etc/shadow文件）进行比对。如果输入的密码匹配成功，系统将确认用户的身份认证成功。
- 授权和访问控制: 例如查看文件、运行程序、管理文件夹等。系统会根据用户的权限来确定允许执行的操作。

身份认证的分类



身份认证可以分为**本地**和**远程**两类

- **本地**：物理接触的情况下进行的身份认证，通常不涉及与网络通信或远程设备的交互通信。
- **远程**：远程身份认证是指通过网络或其他远程通信方法进行的身份认证。包括使用用户名和密码、数字证书等。通常涉及与远程服务器之间的通信。

可以是**单向**的也可以是**双向**的

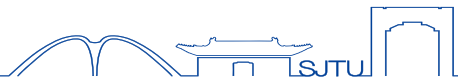
- **单向认证**是指通信双方中只有一方向另一方进行鉴别
- **双向认证**是指通信双方相互进行鉴别

认证协议



- NTLM (NT LAN Manager)
- Kerberos

基于口令的身份认证



一种常见的身份验证方法，要求用户提供一个秘密的字符串（密码）作为身份验证凭证。这个密码必须与存储在系统或服务器中的用户帐户相关联的密码匹配，以便用户能够成功通过认证。

一般流程：

- 用户提供口令：用户在登录时会提供一个口令以证明身份。
- 系统验证口令：系统将用户提供的口令与存储在数据库的相关用户帐户的口令进行比对。通常系统不会存储明文密码，而是存储其**哈希值密文**。
- 成功或失败：如果用户提供的口令与数据库中存储的口令匹配，认证成功，用户可以获得访问权限。如果口令不匹配，认证失败，用户无法获得访问权限。

口令选择和管理



口令格式：

- **使用混合字符：**口令应该包括字母（大小写）、数字和特殊字符（例如！、@、#、\$、%等）。
- **长度足够：**一般建议至少8个字符，以增加安全性。

易记难猜原则：

- 口令应该容易记住，但不容易被猜测。应避免使用过于明显的信息，如生日、姓名、常见单词或短语等。避免连续数字或键盘上相邻的字符。

计算机生成口令：

- 计算机可以生成随机的、强安全性的口令。用户可以使用密码管理工具来生成和存储安全的口令，以避免记忆多个复杂口令。

多因素认证：

- 即使口令被泄露，仍需要额外的身份验证信息才能访问

定期更改口令

Chrome浏览器密码管理工具



口令预检查



在创建或更改用户口令时执行的安全策略，权衡用户友好性和安全性，以防止用户选择过于简单或易于猜测的口令。

强制规则：

- 口令长度不能小于一定值（例如，8个字符）。
- 大写字母、小写字母、数字、特殊字符（例如！、@、#、\$、%等）

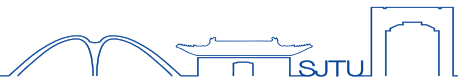
坏口令表（坏口令字典）：

- 坏口令表是一个包含常见弱口令的列表。在口令预检查中，系统会检查用户选择的口令是否在坏口令表中。如果是，系统会拒绝这个口令，要求用户选择一个更安全的口令。

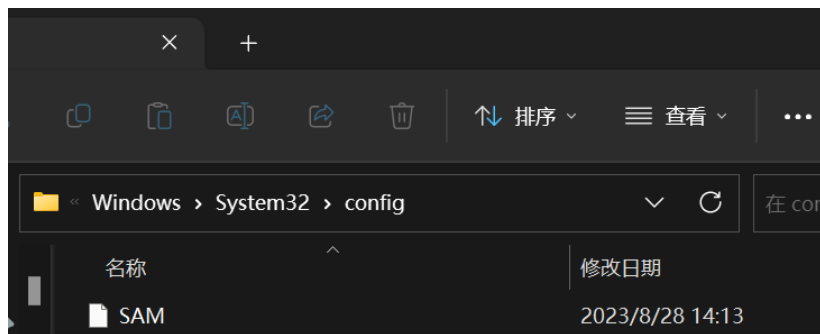
123456、123qwe、qwerty、qweasd、zhang456、wang1998、
admin123、5201314

问题：如何开发出存储开销小、查询快的口令预检查系统？使用合适的数据结构、索引、哈希查找等

口令存储



- 口令一般存储在**口令表**（口令文件）中，包括用户的身份标识（ID）和口令哈希密文。
- Windows的口令信息存放在SAM(Security Account Manager)数据库中。该文件位于C:\Windows\System32\config目录下。包含了本地用户帐户的密码哈希值以及其他信息。（本机sam文件）
- Linux系统存放在/etc/passwd和/etc/shadow文件。



```
-rW-r--r-- 1 root root 2636 Sep 9 07:22 /etc/passwd  
-rW-r----- 1 root shadow 1668 Sep 9 07:57 /etc/shadow
```

口令存储问题



问题：两个用户选择了同样的口令，系统会在口令表中建立两个相同的记录（即便对口令进行加密）。根据密文相同，攻击者会知道其对应的明文也相同

用户名：Alice 密码：Password123

008c70392e3abfbd0fa47bbc2ed96aa99bd49e159727fcb
0f2e6abeb3a9d601

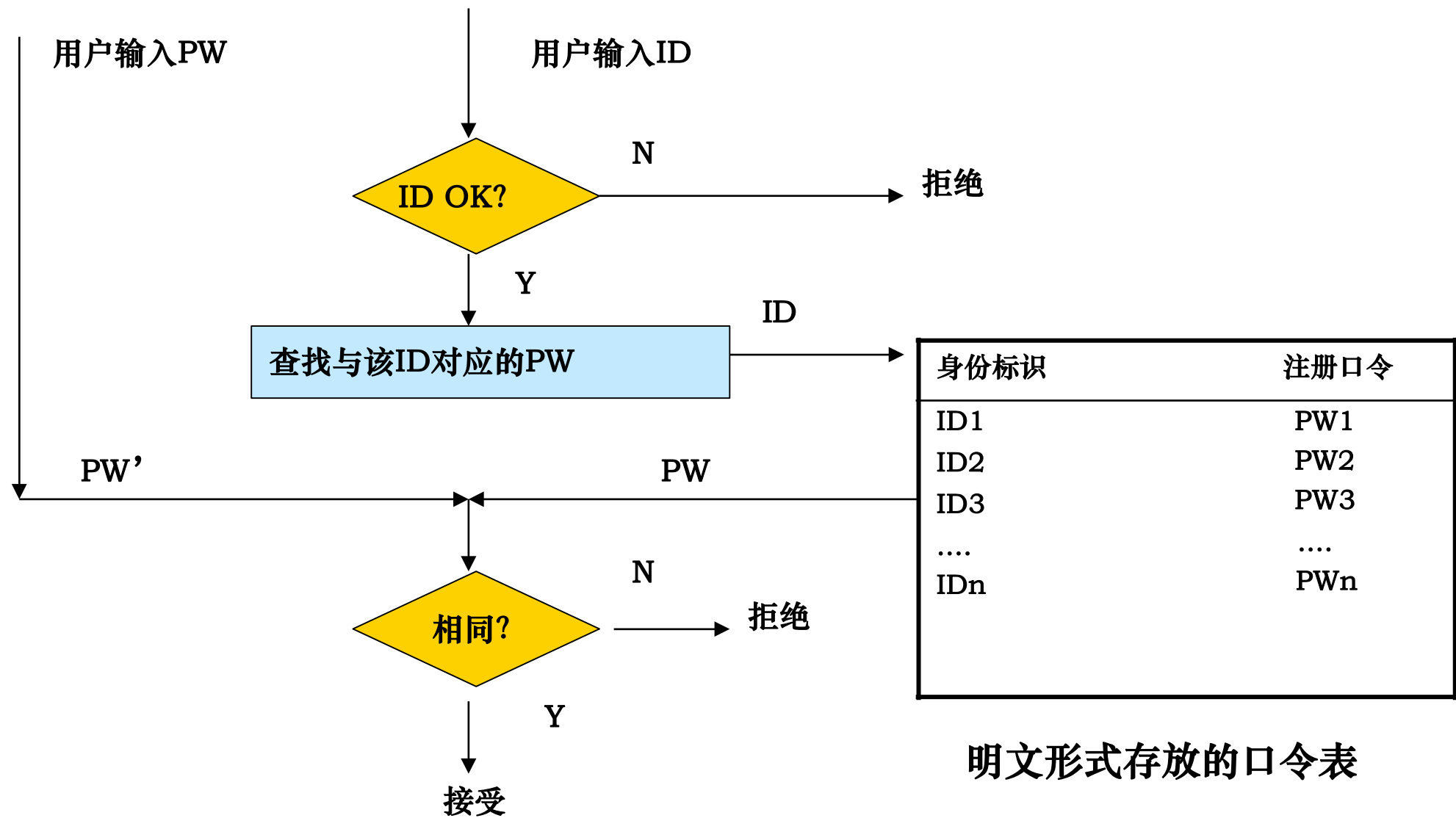
用户名：Bob 密码：Password123

008c70392e3abfbd0fa47bbc2ed96aa99bd49e159727fcb
0f2e6abeb3a9d601

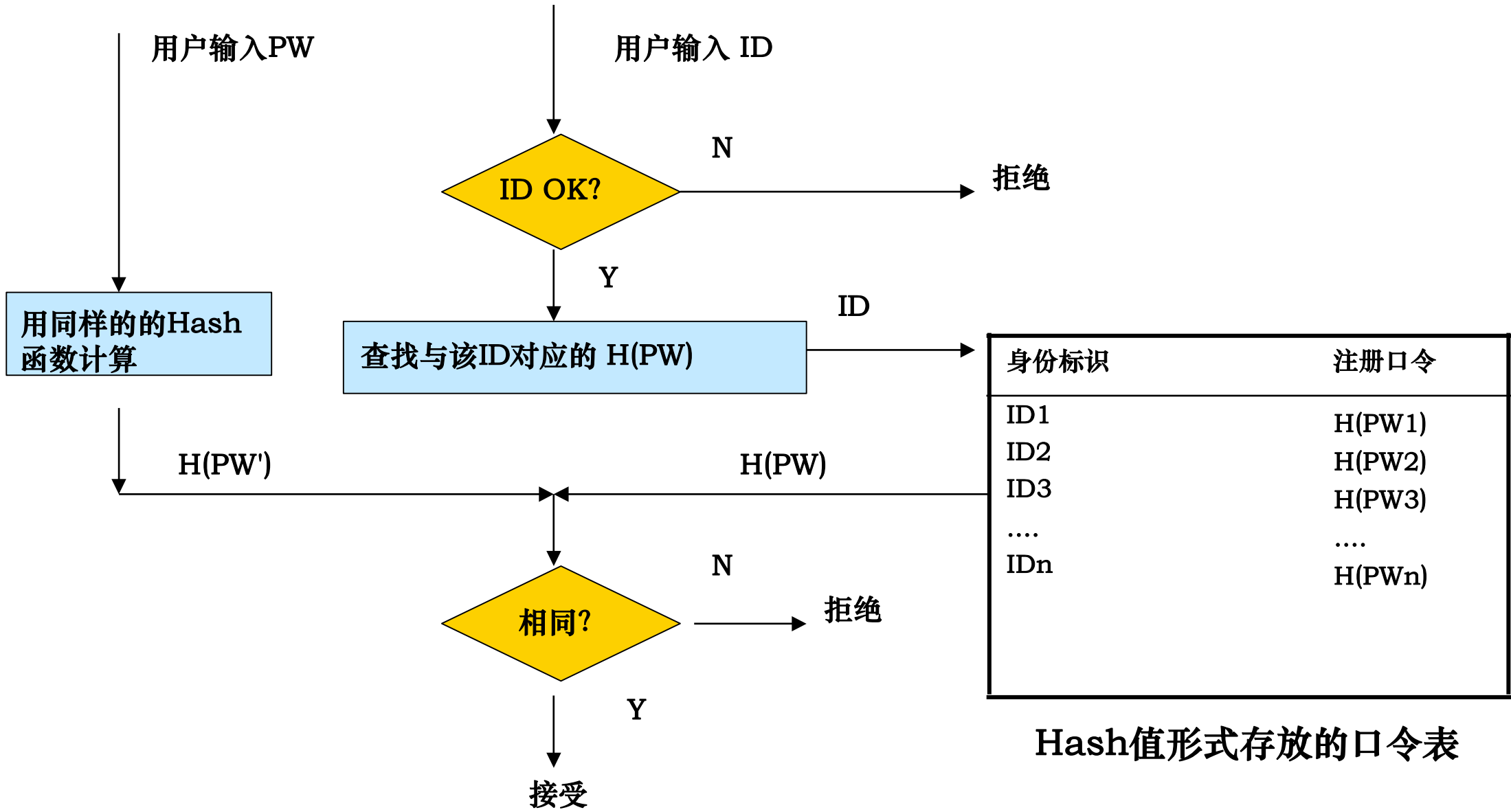
<https://passwordrecovery.io/sha256/>

解决方法：存口令时，在原始口令的基础之上额外增加一些信息(盐)，同时对口令和盐加密，确保口令相同，但密文不同。

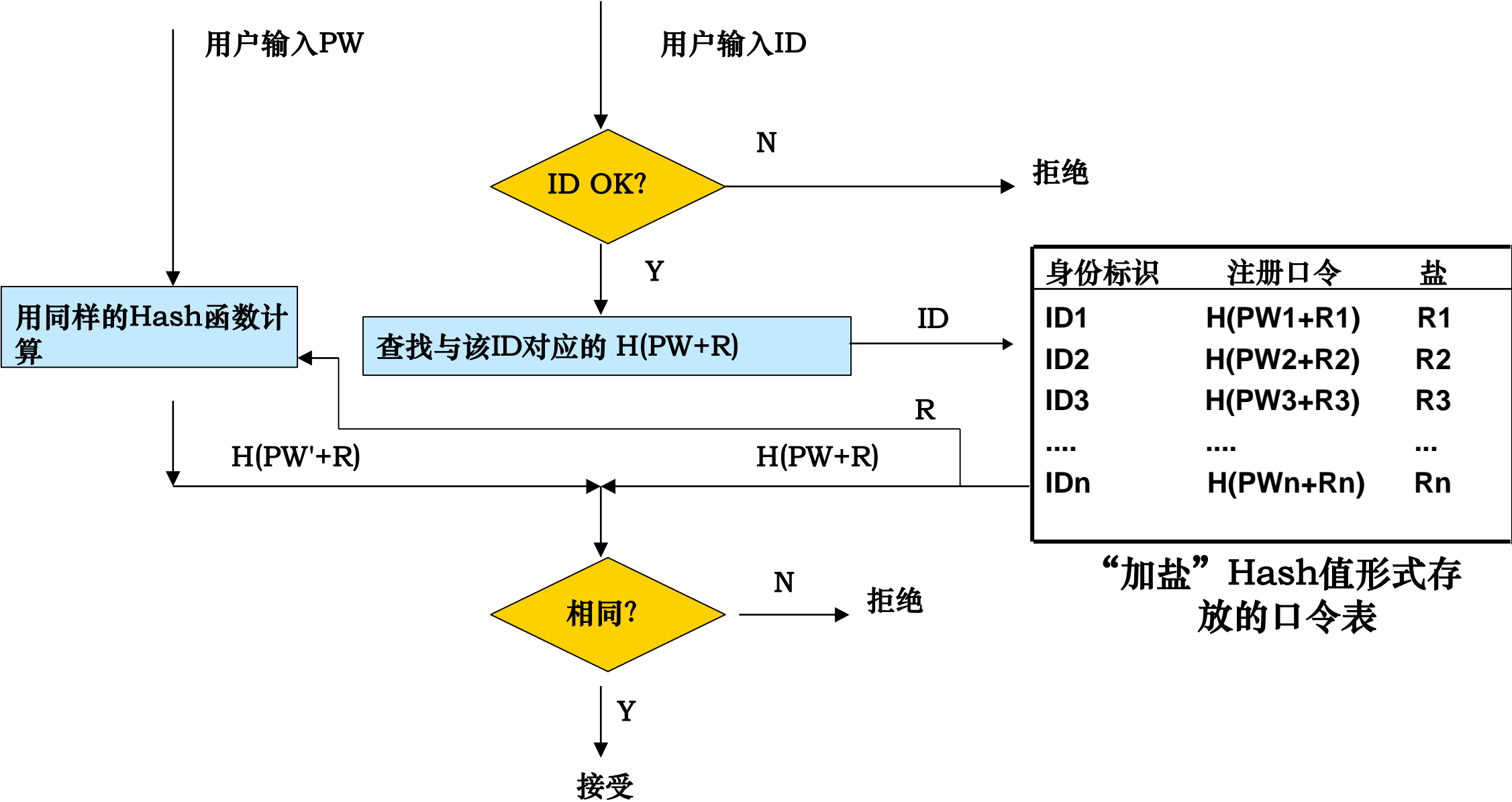
明文口令表



基于单向hash函数的口令表



加盐Hash口令表



基于口令的身份认证面临的威胁



- 通过系统攻击获取口令文件：攻击者可以尝试通过利用操作系统或应用程序的漏洞，获得权限升级，来获取口令文件。
- 通过访问文件系统并拷贝SAM文件：攻击者可以通过某种方式访问包含SAM文件的文件系统，例如使用Windows PE，然后拷贝出SAM文件，然后离线尝试对其中的口令进行破解。
- 获取多个系统上相同的口令：攻击者可以尝试在不同的系统上使用相同的口令，强烈建议用户不要在多个系统上使用相同的口令，因为一旦一个系统受到攻击，其他系统也可能面临风险。



口令安全管理方法



- 使用强密码策略
- 口令定期更改，强制用户定期更改口令
- 多因素认证，要求用户提供除口令之外的其他身份验证因素，如手机验证码
- 使用密码管理工具来生成、存储和自动填写安全的口令
- 定期监控用户的登录活动和口令更改活动，并进行安全审计
- 在发现口令泄露或安全事件时，立即采取措施，例如锁定受影响的帐户
- 定期更新操作系统和应用程序，以修复已知的漏洞，从而减少攻击的风险



信息安全综合实践

Linux安全基础



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY



信息安全综合实践

虚拟机的使用



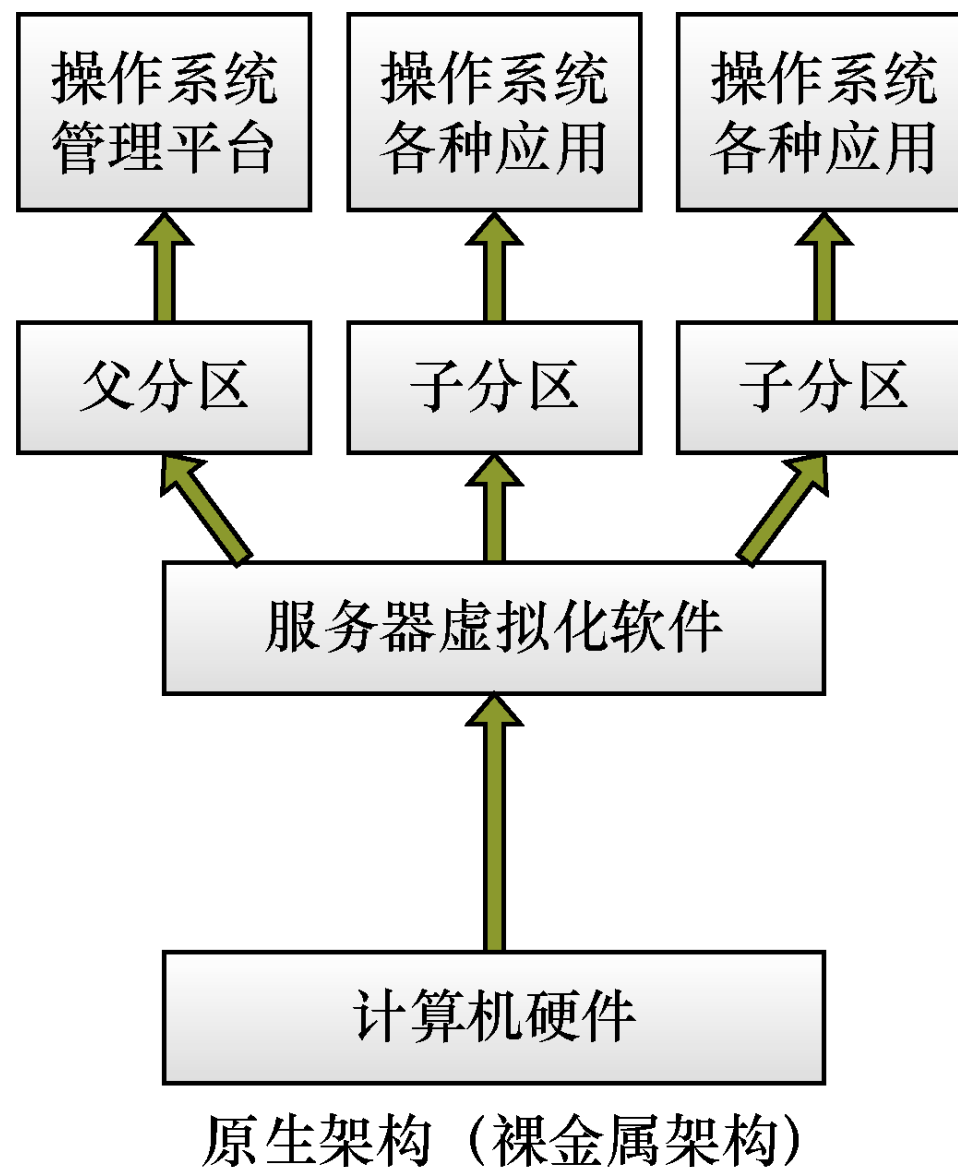
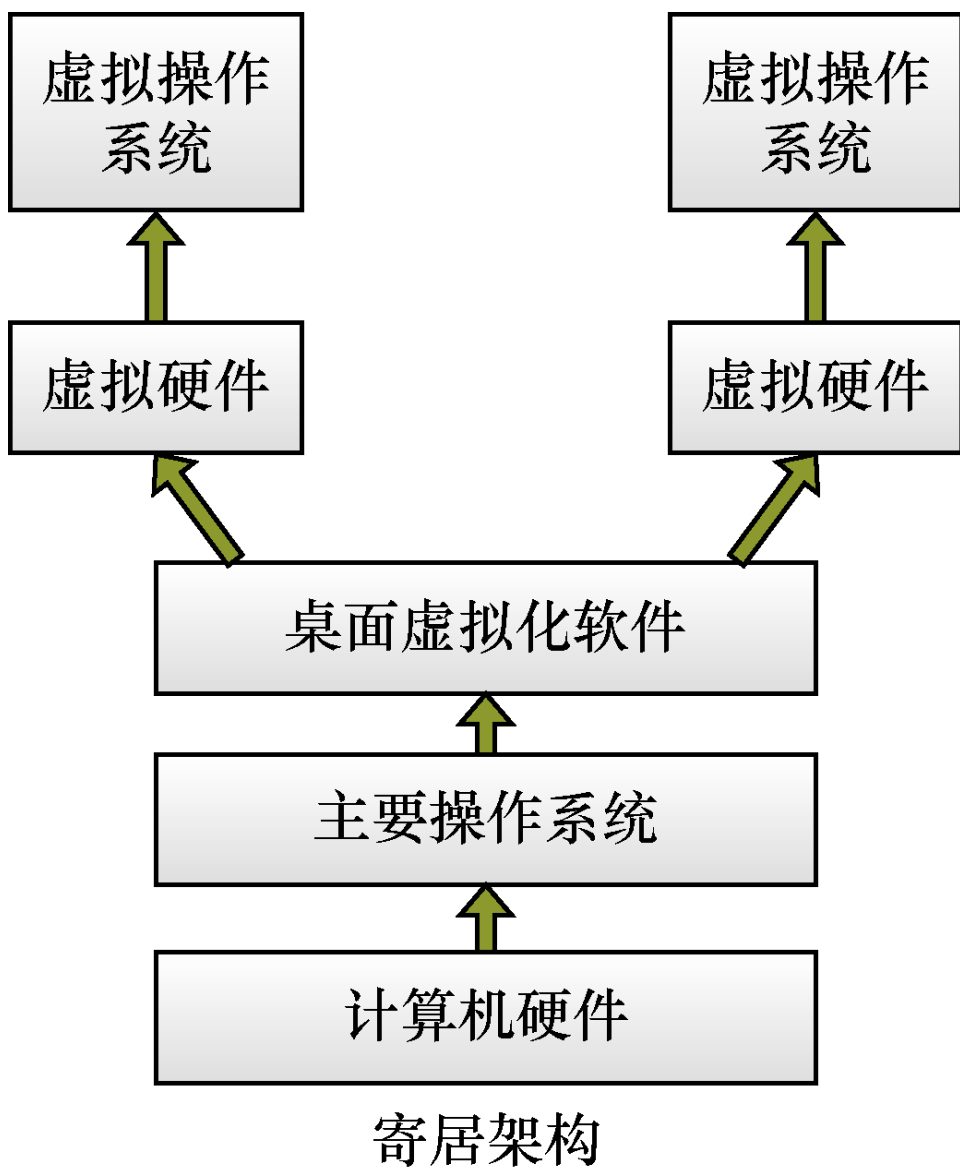
上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

为什么要学习虚拟机的使用



- 在学习使用 Linux 系统的过程中必然要进行大量的实验操作，这些操作离不开虚拟机软件。本课程所有实验操作都是基于虚拟机进行的。
- 目前的虚拟机产品主要分为两个大类
 - 原生架构，有时也称作裸金属架构。直接安装在计算机硬件上，不需要操作系统的支持，它可以直接管理和控制计算机中的所有硬件设备，因而这类虚拟机拥有强大的性能，主要用于生产环境。典型产品就是 vSphere、Citrix，以及 Linux 系统中自带的 KVM。
 - 寄居架构，这类虚拟机必须要安装在操作系统上，通过操作系统去调用计算机中的硬件资源，主要用于教学或学习。典型产品是 Vmware Workstation 和 VirtualBOX

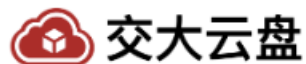
寄居架构和裸金属架构



Vmware Workstation的安装



- 建议的硬件配置
内存：8GB及以上
硬盘：固态硬盘SSD
- 下载镜像，例如Ubuntu、Kali
- <https://jbox.sjtu.edu.cn/1/z1fMJq>



铭的分享

转存至网盘

保存到手机

☐ 文件名

|| 更新时间 (人) ◆

|| 大小

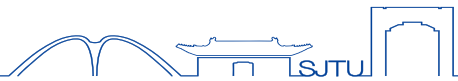


☐ 信息安全综合实践虚拟机

2023-08-18 23:36 | 铭

-

NAT网络模式



- VMware中的**NAT**（Network Address Translation，网络地址转换）网络模式是一种用于虚拟机网络连接的配置选项。
- NAT网络模式允许虚拟机通过虚拟网络适配器与外部网络通信，同时提供了一定程度的网络隔离和安全性。
- VMware中虚拟机的网络设置为NAT模式，虚拟机可以自动接入到Internet。



UNIX 系统



- 贝尔实验室中有一位名为 Ken Thompson 的工程师1970开发的。
- 1970 年定为 UNIX 元年，并且在 UNIX 系统中将 1970 年 1 月 1 日 0:00 作为计算机时间的起点。
- 随着 UNIX 系统的不断发展，逐渐出现了一些商业化的 UNIX 版本，如美国加州大学伯克利分校开发的BSD、IBM 公司开发的 AIX 以及 HP 公司推出的 HP-UX 等。
- 贝尔实验室收回了 UNIX 系统的版权，而且各个商业化版本的 UNIX 系统价格不菲，因此荷兰 Vrije 大学讲授“操作系统原理”课程的 Andrew S. Tanenbaum 教授在 1987 年仿照 UNIX 自行设计了MINIX，专门用于教学。MINIX 系统是免费的，功能非常简单，而 Tanenbaum 教授为了保持系统代码的纯洁性，拒绝了人们对 MINIX 功能进行扩展的要求。



Linux 系统



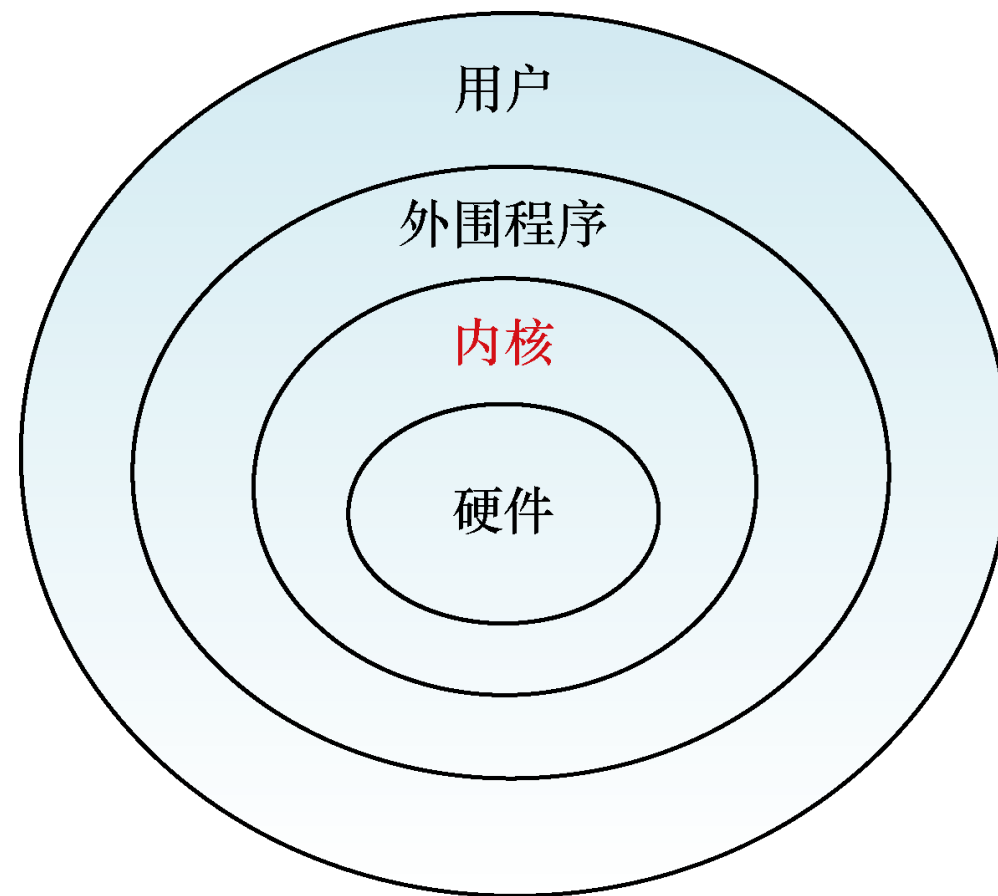
- 芬兰赫尔辛基大学的学生 Linus Torvalds 在 MINIX 系统的基础上，增加了很多功能使之完善，并于 1991 年将修改之后的系统发布在互联网上，被称为 Linux 系统。
- Linux 系统采用市集式（Bazaar）的开发模式，任何人都可以参与其开发及修正的工作。



Linux Kernel



- 内核直接运行在计算机硬件之上，管理计算机中的硬件设备，它是所有上层程序运行的基础
- Linux 系统中的内核程序被称为 Kernel
- 从 Linux Kernel 的官方网站中可以下载已发布的每一个版本的 Kernel 程序
- [The Linux Kernel Archives](#)



Linux 的发行版本



- RedHat Linux



红帽企业系统 (RedHat Enterprise Linux, RHEL.)

全球最大的开源技术厂商之一，全世界使用最广泛的Linux发布套件之一，提供性能与稳定性极强的Linux套件系统并拥有完善的全球技术支持。

- CentOS



- Debian



Linux系统的图形界面和字符界面



- Linux系统安装完成后，默认会进入图形界面下的桌面环境。Linux系统的桌面环境（称为X Window）是由应用软件来提供的。
- 虽然图形界面提供了更为友好的操作方式，但 X Window 只是Linux 系统中的一个应用软件，并没有集成到 Linux 的内核中
- 虽然图形界面操作简单，但是需要占用更多的系统资源，而字符界面的效率则要高得多。因此，在学习 Linux 系统的过程中，要以学习字符界面中的操作为主。

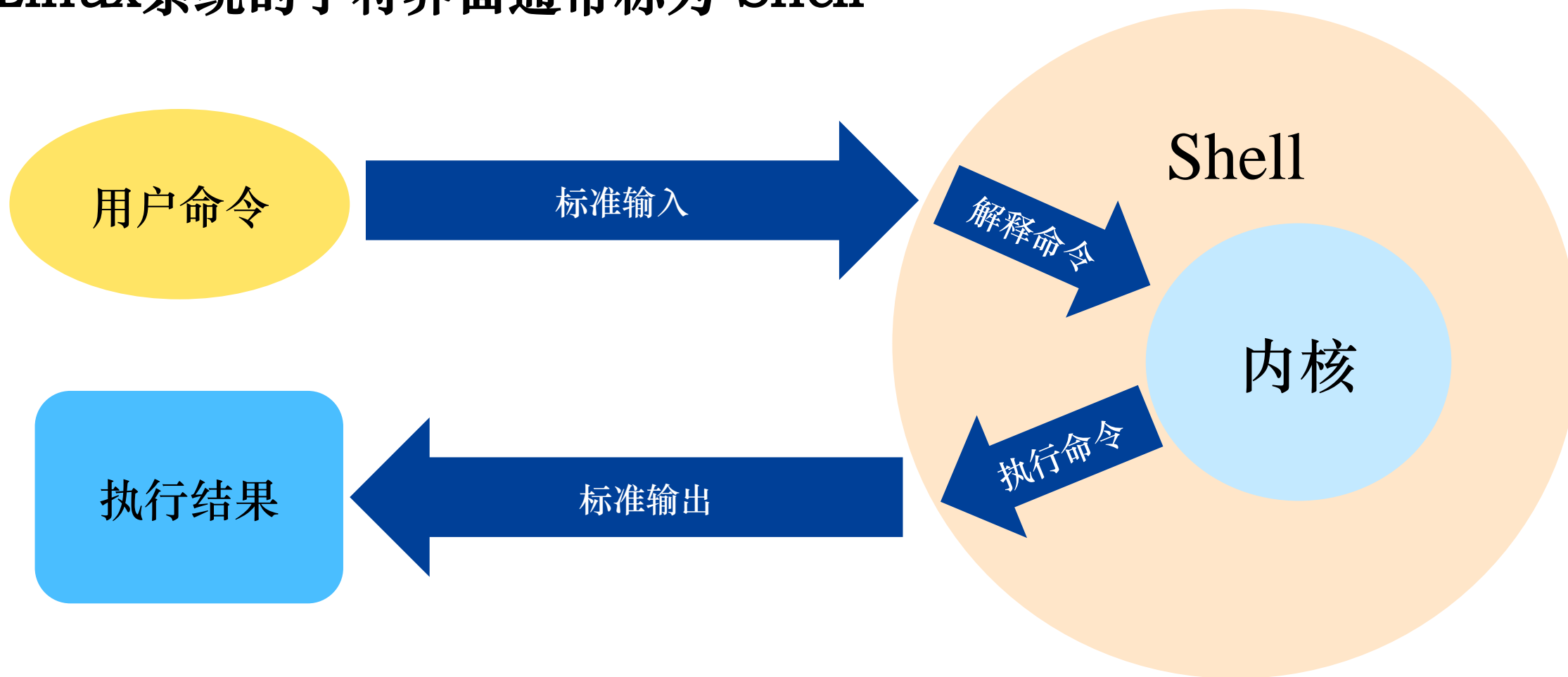
NAME

X - a portable, network-transparent window system

Shell



- Linux系统的字符界面通常称为 Shell



Shell和Terminal



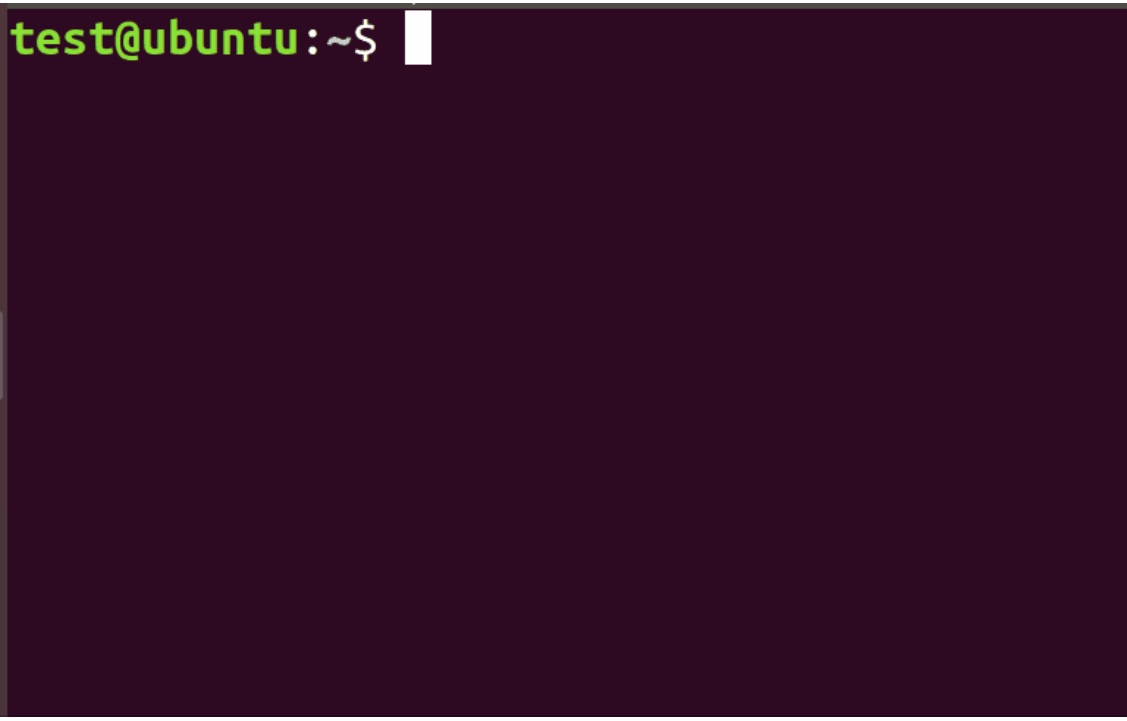
- Shell是操作系统中的一个程序，负责解释用户输入的命令并将其转换为操作系统可以理解的指令。操作系统执行这些指令。
 - Shell还可以执行脚本文件，从而批量执行一系列命令。
 - 常见的Shell包括bash、sh、csh等。
 - Windows系统中的命令提示符（Command Prompt）也可以视为一种Shell。
- Terminal是访问操作系统的Shell的接口
 - 任何一个可以输入命令的交互式接口，都可以称为终端
 - pts

```
root@ubuntu:/home/test# tty  
/dev/pts/1
```

命令提示符



- 启动 Shell 之后，首先可以看到类似于 “test@ubuntu:~\$” 的命令提示符。
- 命令提示符是 Linux 字符界面的标志，其中的 “test” 表示当前登录的用户账户名；
- “ubuntu” 表示本机的主机名； “~” 表示用户当前所在的位置，也就是工作目录， “~” 泛指用户的家目录，
/home/test
- 最后的 “\$” 字符表示普通用户



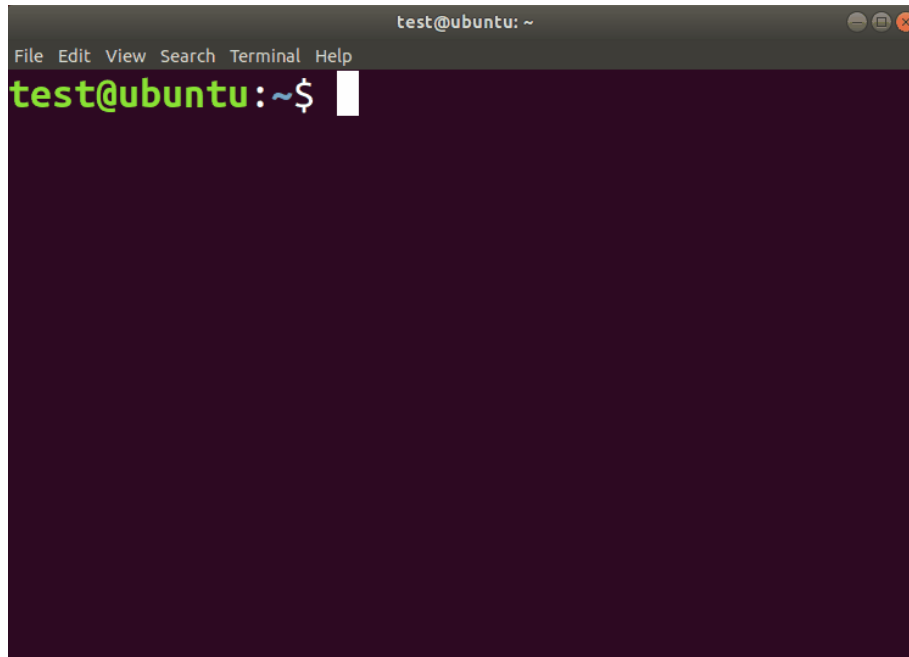
```
test@ubuntu:~$
```

管理员用户



- 其中的“root”表示当前登录的用户是管理员
- “~”表示用户当前所在的位置，也就是工作目录，“~”是一个特殊符号，泛指用户的家目录，root 用户的家目录就是/root
- 最后的“#”字符表示当前登录的是管理员用户

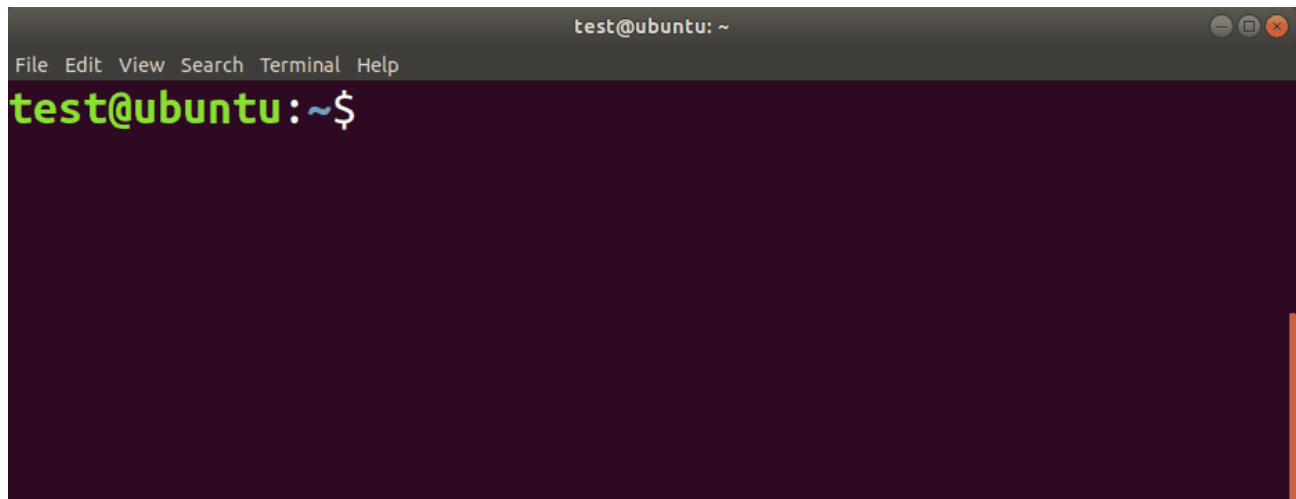
```
root@ubuntu:~#
```



关机与重启命令



- `poweroff` #关机
- `reboot` #重启
- 除这两个命令之外，`shutdown` 命令也可以实现关机与重启的功能
 - 立即关闭系统
 - `shutdown -h now`
 - 立即重启系统
 - `shutdown -r now`
- 相比于 `poweroff` 和 `reboot` 命令，`shutdown` 命令在关闭或重启系统之前会给所有登录用户发送警告信息，因而要更加安全

A screenshot of a terminal window titled 'test@ubuntu: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The prompt 'test@ubuntu: ~\$' is visible on a dark purple background.

cd命令



- `cd ~` #回到用户的家目录
- `cd #`不加任何参数，回到用户的家目录
- `cd ..`回到上级目录

```
root@ubuntu:/#
```



信息安全综合实践

Linux的文件和目录管理



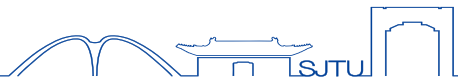
上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

Linux一切皆文件

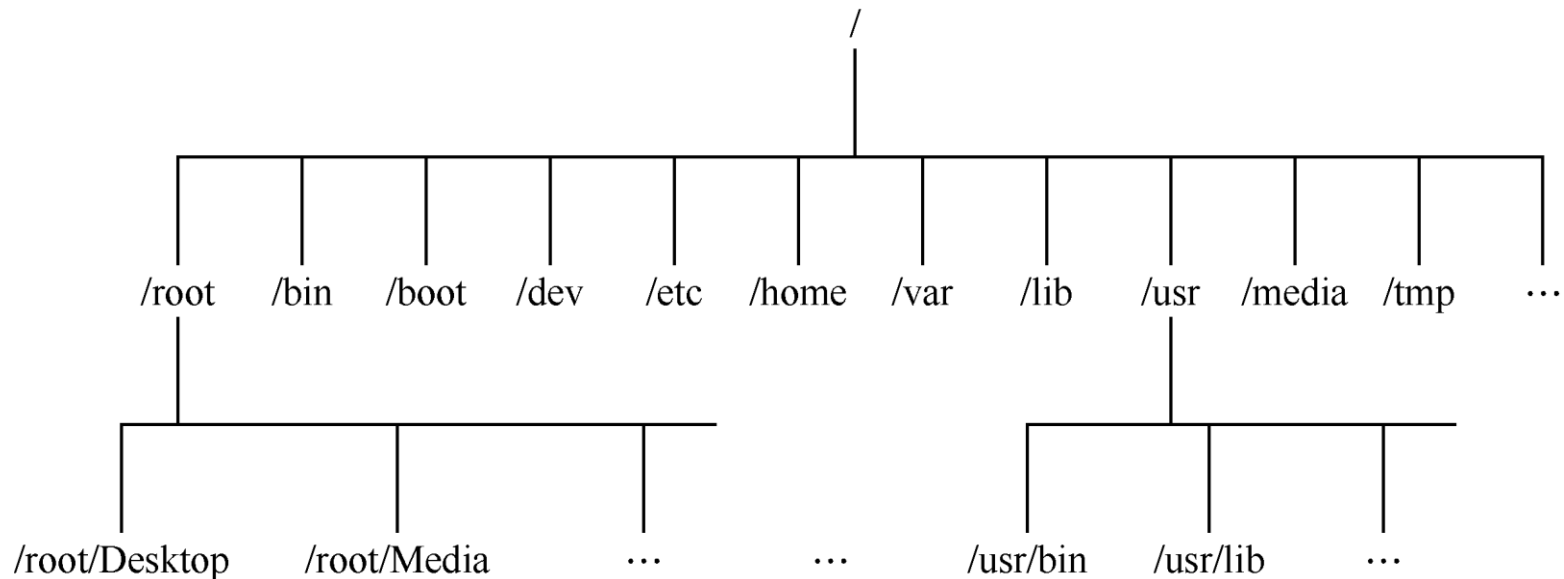


- “Linux 一切皆文件”（“Everything is a file”）是类Unix操作系统的一种思想。数据、系统资源和设备都被视为文件，并且可以通过文件操作的方式来进行访问和管理。
- 并不是字面上的“文件”，而是将资源和设备抽象为了文件的形式。
 - 统一性：不同类型的数据和资源都可以通过相同的文件操作接口来处理，并可以通过文件系统路径进行定位。
 - 可扩展性：如果新的硬件或资源被引入，可以很容易地将其表示为文件来扩展。

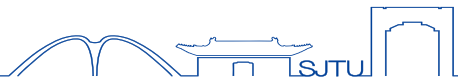
Linux的目录结构



- 在Windows系统中通过盘符访问分区，如C盘，D盘，每个分区使用独立的文件系统，每一个分区中都有一个根目录,如C:\ D:\等。
- Linux系统的目录结构是一种统一的、层次化的树形文件系统结构，以一个根目录（/）为起点，系统中的文件、目录和设备按照特定的组织方式进行分类和排列。



Linux常用目录



- /boot: 存放 Linux 系统启动所必需的文件， Kernel 被存放在这个目录中
- /etc: 存放 Linux 系统和各种程序的配置文件， Linux 中的很多操作和配置都是通过修改配置文件实现的
- /dev: 存放 Linux 系统中的硬盘、光驱和鼠标等硬件设备文件
- /bin: 存放 Linux 系统中常用的基本命令，任何用户都有权限执行
- /home: 普通用户家目录（也称为主目录）。例如，用户账号“student”对应的家目录位于“/home/student”
- /root: 超级用户 root 的家目录

绝对路径和相对路径



假设当前用户的用户名为 “student”

- 绝对路径：从根目录开始到指定文件的完整路径
 - `/home/student/Documents/file.txt`
- 相对路径：相对于终端的当前目录的路径
 - 假设当前位于 `/home/student/` 目录，要指向 `file.txt`，那么相对路径就是 `Documents/file.txt`
- 建议在初始时尽量使用绝对路径，以便于理解和区分

文件和目录的操作命令：pwd命令



- pwd (print working directory) ，该命令用于显示用户当前所在的工作目录路径。使用 pwd 命令可以不添加任何选项或参数。
- 例如在命令提示符后面直接执行 pwd 命令，可以看到用户当前所在的工作目录为 “/home/test” 或 “/root”

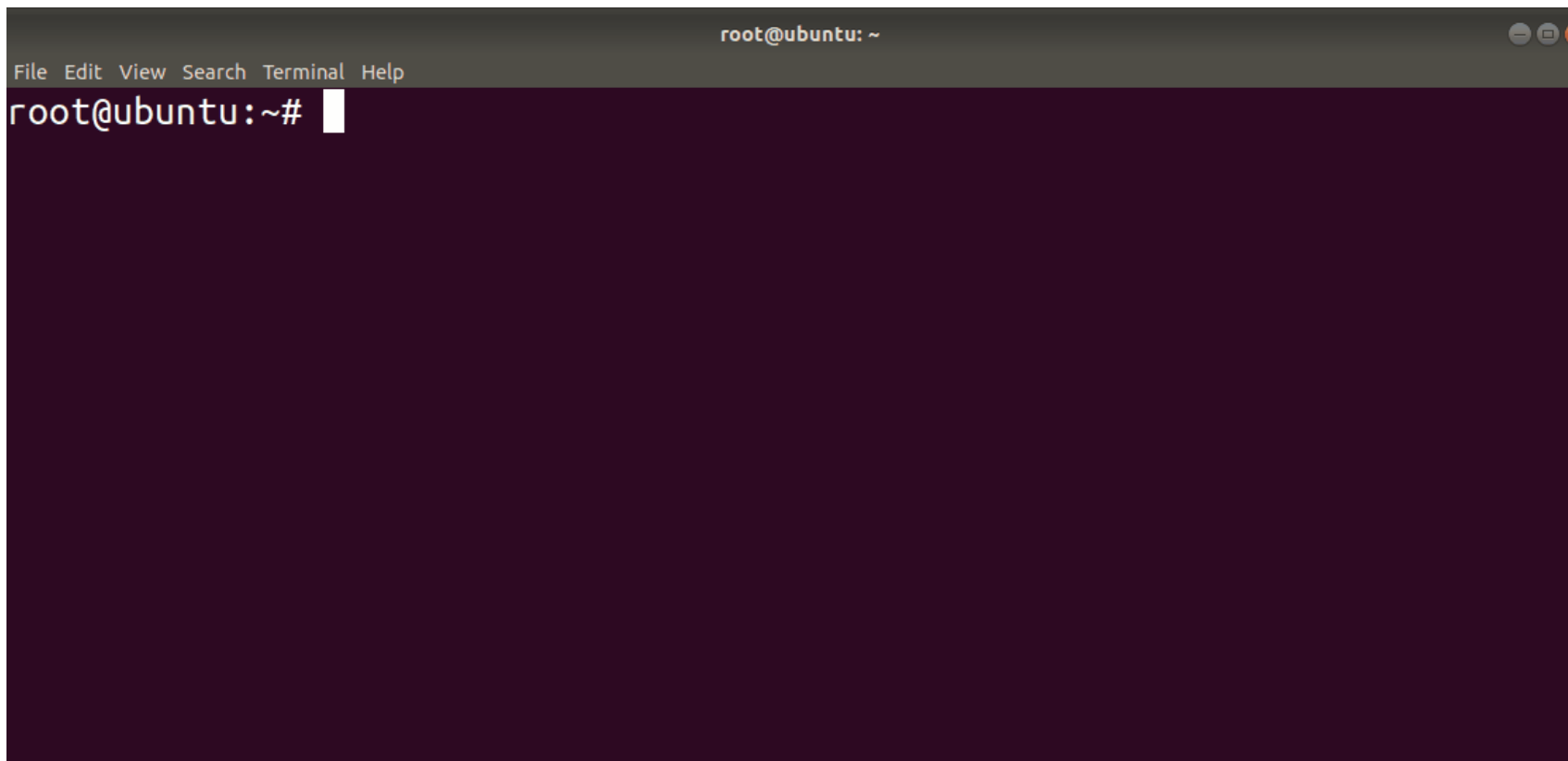
```
test@ubuntu: ~  
File Edit View Search Terminal Help  
test@ubuntu:~$
```

```
root@ubuntu: ~  
File Edit View Search Terminal Help  
root@ubuntu:~#
```

ls命令—列表显示



- `ls -al` 或 `ll -a`
- “-a” 选项，显示所有文件，包括隐藏文件。
- “-l” 选项，以长格式（内容更详细）显示文件或目录的详细信息。

A screenshot of a terminal window with a dark purple background. The title bar at the top reads 'root@ubuntu: ~' and includes standard window control buttons. Below the title bar is a menu bar with the options 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The main area of the terminal shows the prompt 'root@ubuntu:~#' followed by a white cursor. The rest of the terminal area is empty.

ls -al命令的结果



```
test@ubuntu:~$ ls -al
total 80
drwxr-xr-x 15 test test 4096 Aug 30 08:47 /
drwxr-xr-x  4 root root 4096 Aug 30 05:02 /usr
-rw-r--r--  1 test test 1650 Sep  8 23:11 /etc/passwd
-rw-r--r--  1 test test  220 May 22 17:28 /etc/passwd.bak
-rw-r--r--  1 test test 5771 May 22 17:28 .bashrc
drwx----- 14 test test 4096 Aug 25 03:29 /home
drwx----- 11 test test 4096 May 22 17:33 .config
drwxr-xr-x  2 test test 4096 May 22 17:32 Desktop
drwxr-xr-x  2 test test 4096 May 22 17:32 Documents
drwxr-xr-x  2 test test 4096 May 22 17:32 Downloads
drwx-----  3 test test 4096 May 22 17:32 .gnupg
-rw-r--r--  1 test test 2862 Aug 30 08:39 .ICEauthority
drwx-----  2 test test 4096 Aug 30 08:47 .john
drwx-----  3 test test 4096 May 22 17:32 .local
drwxr-xr-x  2 test test 4096 May 22 17:32 Music
drwxr-xr-x  2 test test 4096 May 22 17:32 Pictures
-rw-r--r--  1 test test  807 May 22 17:28 .profile
drwxr-xr-x  2 test test 4096 May 22 17:32 Public
-rw-r--r--  1 test test    0 May 22 17:33 .sudo_as_admin_successful
drwxr-xr-x  2 test test 4096 May 22 17:32 Templates
drwxr-xr-x  2 test test 4096 May 22 17:32 Videos
```

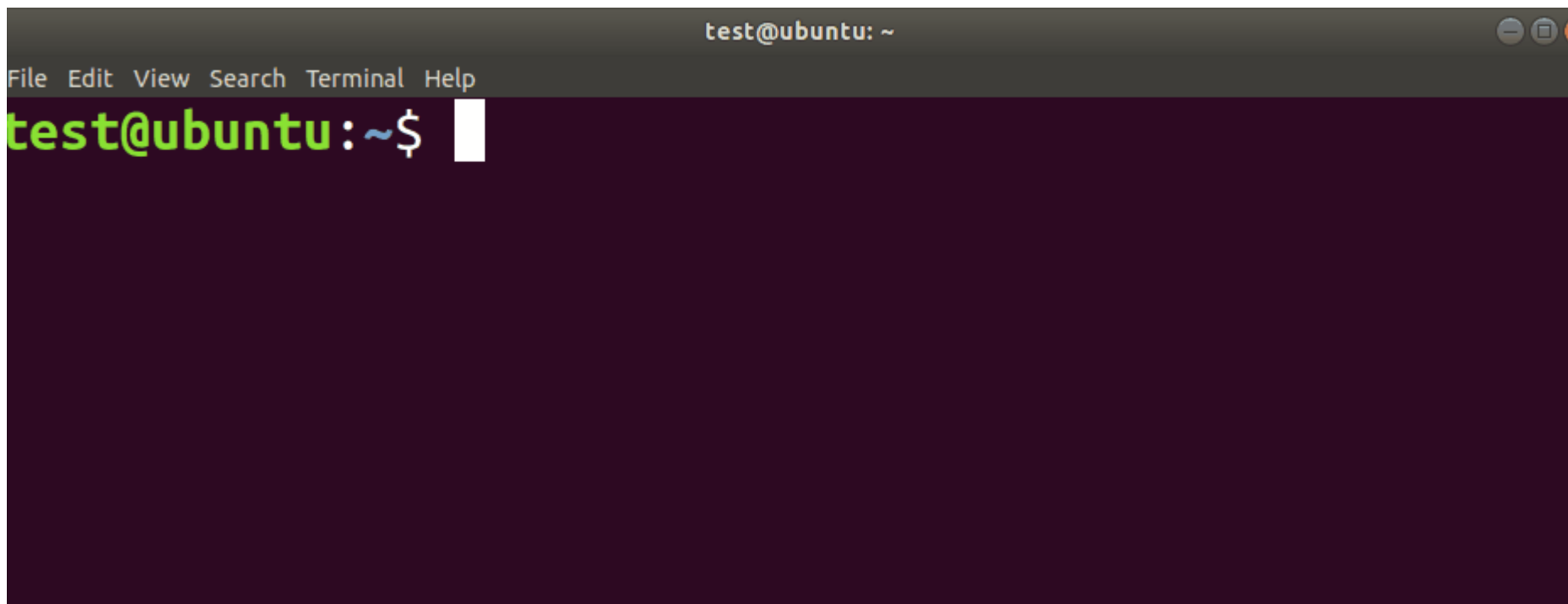
文件目录
系统目录
所有文件

文件名称，以圆点开头的文件为隐藏文件

touch 命令-创建空文件



- touch 命令用于创建空文件或修改已有文件的时间戳。
- 如果所输入的文件名不存在，那么就会创建相应的空文件。
- 如果 touch 命令中所指定的文件已存在，那么就会将文件的时间戳更新为系统当前时间。例如，在当前目录下创建名为 test1 的空文件。



mkdir命令-创建目录



在当前目录中创建名为 test 的子目录。

- `mkdir test`

在根目录中创建名为 public 的子目录。

- `mkdir /public`

`rmdir` 命令—删除空目录。系统中提供了功能更为强大的 `rm` 命令，因此 `rmdir` 命令在实践中用的并不是太多。

cp命令—复制文件或目录



- `cp [选项] 源文件或目录 目标文件或目录`

如果目标文件不存在，那么将生成新的文件。如果目标文件已存在，那么将覆盖目标文件。

- `cp /etc/fstab /tmp/test.txt`
- `cp /etc/issue /tmp/test.txt`
- “-r” 选项，复制目录时必须使用此选项，表示递归复制所有文件及子目录。

mv命令—移动文件或目录



将 /root/test 目录中的文件 test1.txt 改名为 test2.txt。

- `mv /root/test/test1.txt /root/test/test2.txt`

将文件 /root/test/test2.txt 移动到 /tmp 目录中。

- `mv /root/test/test2.txt /tmp/`

mv 命令的用法与 cp 命令基本类似，但需要注意的是，如果 mv 命令移动的对象是一个目录，并不需要像 cp 命令那样加上“-r”选项，而是可以直接移动。例如，将 /tmp/student 目录移动到 /root 目录中。

- `mv /tmp/student /root/`

rm命令——删除文件或目录



无论删除文件还是删除目录，多数是用 `rm` (`remove`) 命令。例如，将 `/tmp` 目录中的 `test2.txt` 文件删除。

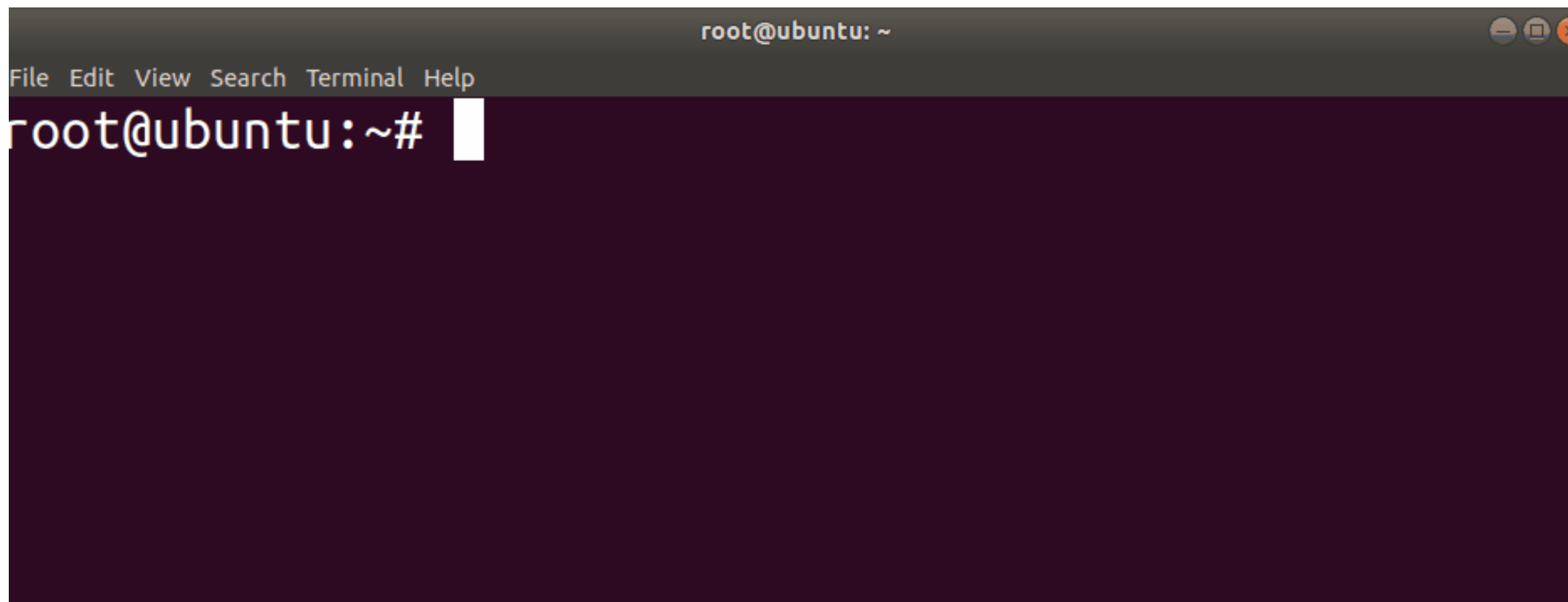
- `rm /tmp/test2.txt`
- “`-r`” 选项，删除目录时必须使用此选项，表示递归删除整个目录

在生产环境中，如果要删除某个文件或目录，建议先用 `mv` 命令将它们移动到某个专门设置的回收目录中，过一段时间之后，确认不再需要这些文件或目录，再用 `rm` 命令将其彻底删除。

命令或路径补全



在输入命令或路径时，如果无法记住完整的命令或路径，可以使用<Tab>键对命令或路径自动补全，以简化输入。

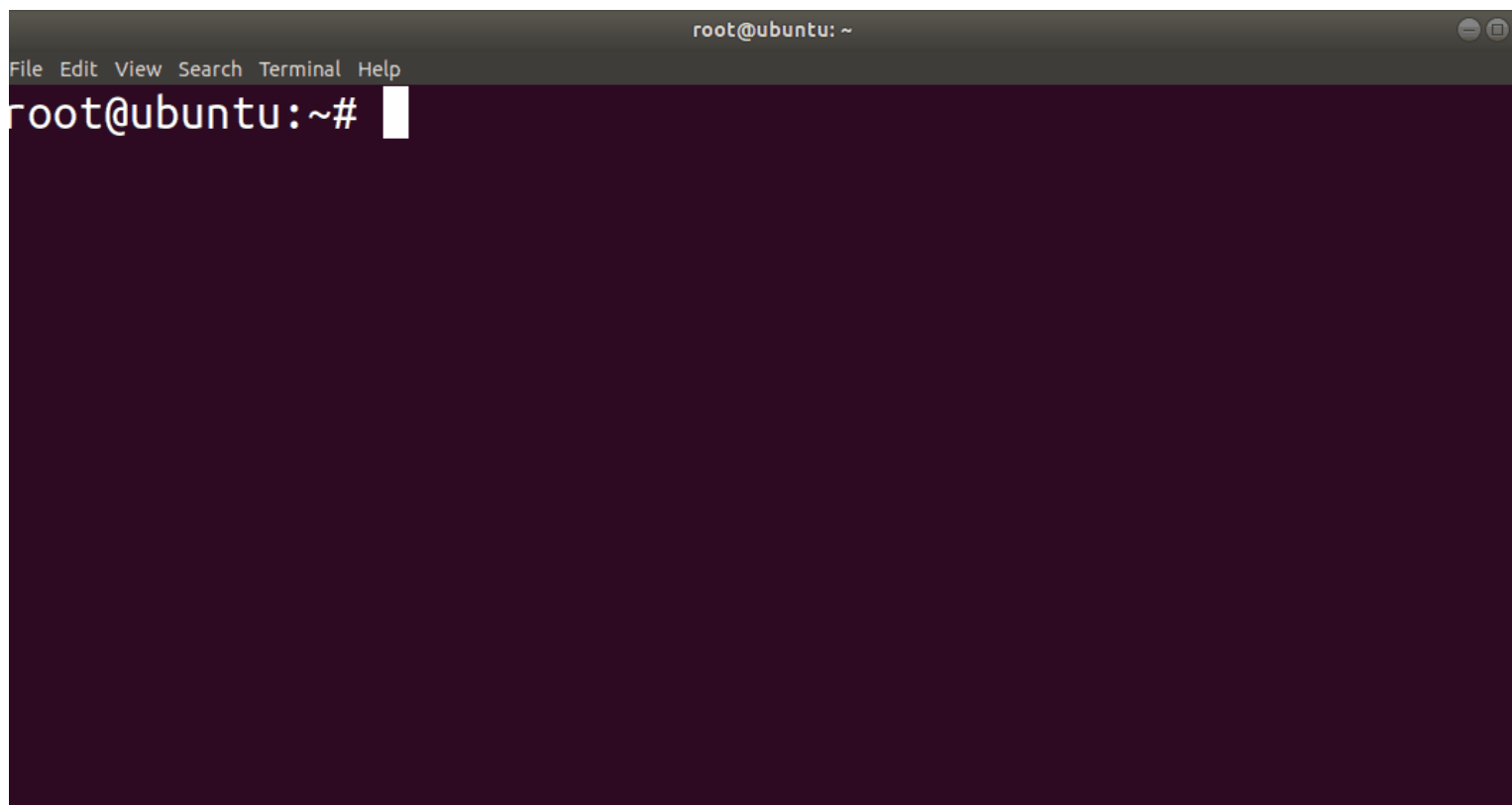


文件内容操作命令:cat 命令—显示文本文件的内容



例如，查看/etc/passwd 文件中的内容，了解 Linux 系统中的用户信息

- `cat -n /etc/passwd`

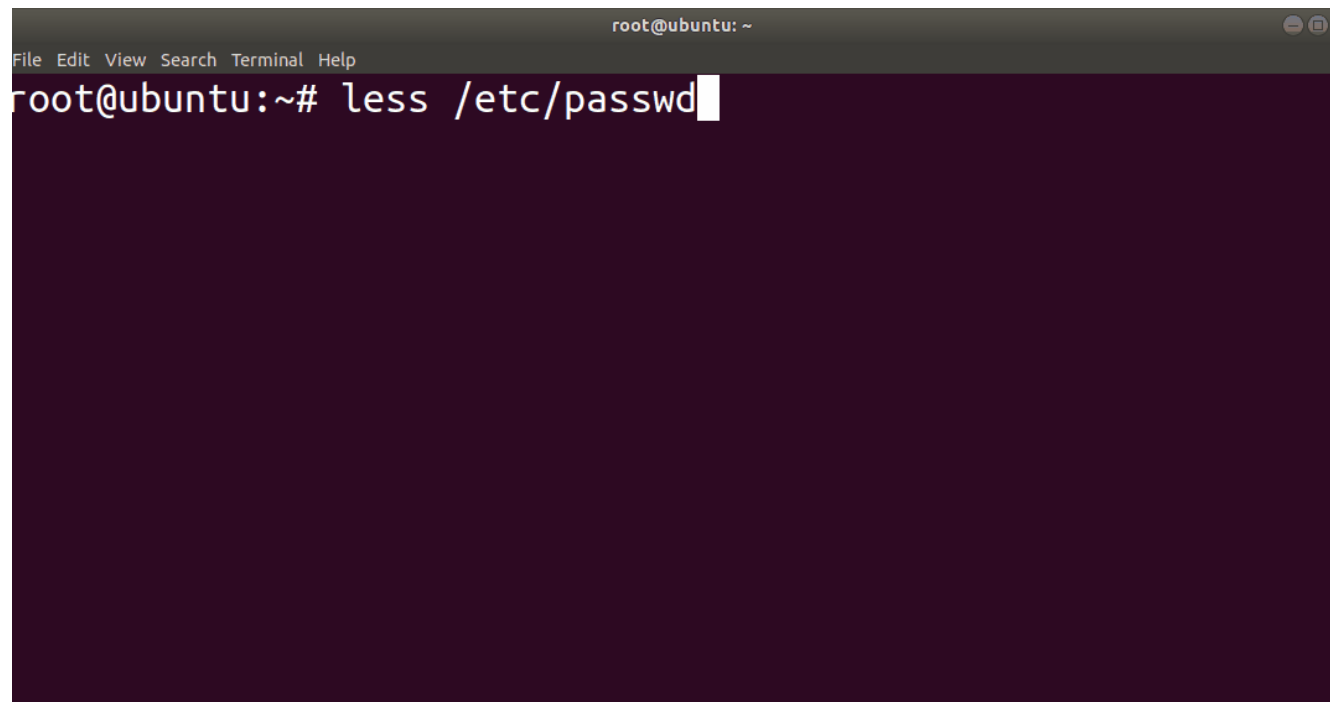
A screenshot of a Linux terminal window. The window title is 'root@ubuntu: ~'. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The command prompt shows 'root@ubuntu:~#' with a white cursor. The terminal background is dark purple, and the text is white. The command 'cat -n /etc/passwd' has been entered but not yet executed.

```
root@ubuntu: ~  
File Edit View Search Terminal Help  
root@ubuntu:~#
```

more 命令和 less 命令——分页显示文件内容



- 使用 more 命令和 less 命令可以进入阅读模式，采用全屏的方式分页显示文件内容，按<Q>键退出，因此更适合用来阅读长文件。
- less 和 more 命令之间的区别：less 命令可以前后翻页，more 命令只能向后翻页；less 命令更有利于对文件内容进行反复阅读。

A screenshot of a terminal window on an Ubuntu system. The window title is 'root@ubuntu: ~'. The menu bar shows 'File Edit View Search Terminal Help'. The command prompt is 'root@ubuntu:~#'. The command 'less /etc/passwd' has been entered, and a white cursor is visible at the end of the command. The terminal background is dark purple, and the text is white.

```
root@ubuntu: ~  
File Edit View Search Terminal Help  
root@ubuntu:~# less /etc/passwd
```

echo 命令—输出指定内容



echo 命令通常用于输出指定的字符串或者变量的值。例如，在屏幕上输出“Hello World”。

- `echo "Hello World"`

在 Linux 系统中有一类由系统定义的变量，称为环境变量。环境变量通常采用大写。例如，SHELL 变量里存放系统当前所使用的 Shell。

- `echo $SHELL`

重定向符号“>”可以将 echo 输出的内容覆盖保存到指定的文件中

重定向符号“>>”可以将 echo 输出的内容追加保存到指定的文件中

- 例如，创建一个名为 1.txt 的文件，文件内容为“a”。

- `echo 'a' > 1.txt`

- 向 1.txt 文件中追加内容“aa” “AAA”。

- `echo 'aa' >> 1.txt`

- `echo 'AAA' >> 1.txt`

echo 命令—输出指定内容



```
root@ubuntu:~#
```


grep 命令——文件内容查找



“-w” 选项，精确匹配单词

```
grep -w AAA 1.txt
```

```
root@ubuntu:~# grep -w AAA 1.txt
AAA
root@ubuntu:~#
```

history 命令——查看命令历史记录



```
root@ubuntu:~#
```

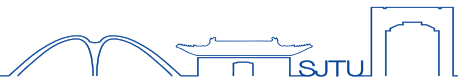
管道符 “|”



通过管道符 “|”，可以把多个简单的命令连接起来以实现更加复杂的功能。管道符 “|” 用于连接左右两个命令，将 “|” 左边命令的执行结果作为 “|” 右边命令的输入，这样 “|” 就像一根管道一样连接着左右两条命令，并在管道中实现数据从左至右的传输。

```
root@ubuntu:~# history | grep echo
68  echo "hello world"
69  echo 'hello world!' > test.txt
70  echo 'hello world2' >> test.txt
71  echo $SHELL
568 echo "Hello World!"
569 echo $SHELL
570 echo a > 1.txt
571 echo aa >> 1.txt
572 echo AAA >> 1.txt
577 history | grep echo
582 history | grep echo
```

Vi 编辑器的使用

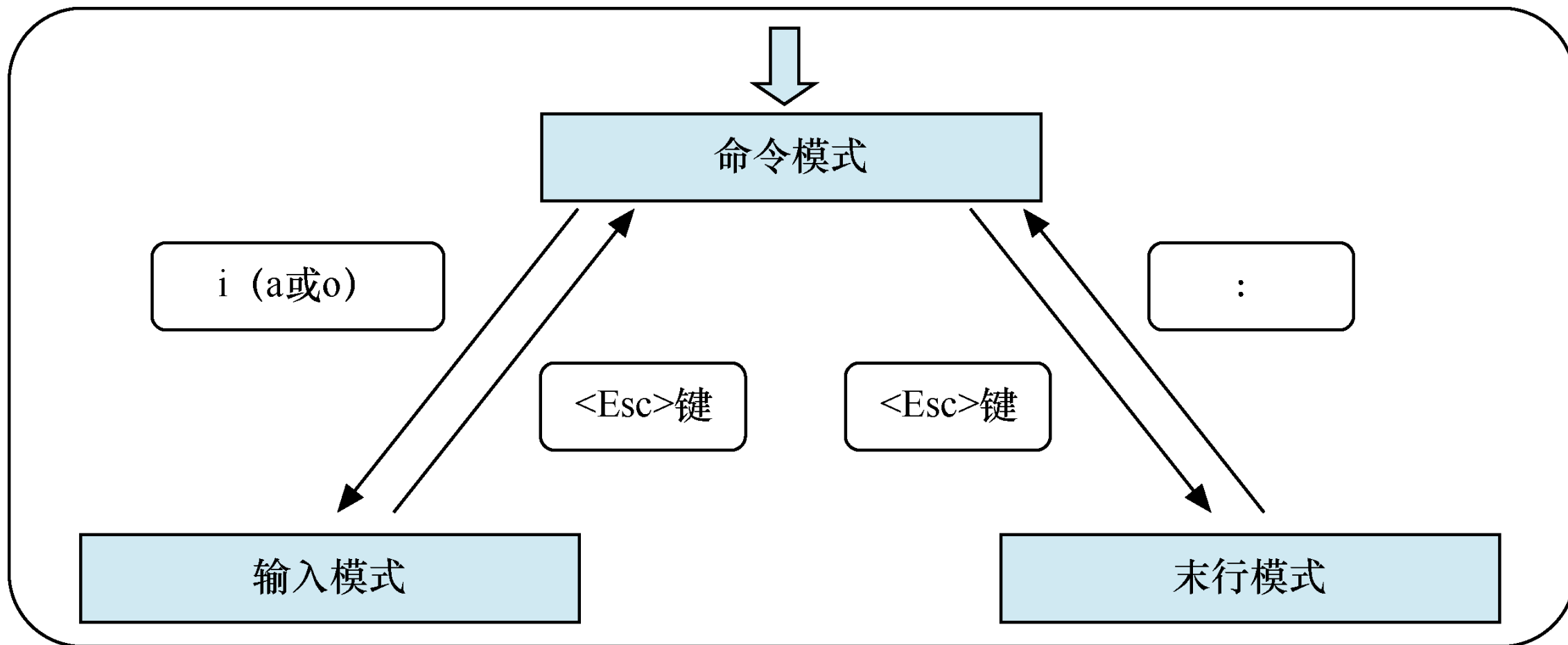


- Vi 是 Linux 系统中使用极为广泛的文本编辑器。nano, gedit
- Vi 是一个基于 Shell 的全屏幕文本编辑器，全部操作都基于命令。
- Vim是 Vi 编辑器的增强版本， 实际上我们平常使用的大多是 Vim。
 - 命令模式。启动 Vi 编辑器后默认进入命令模式，主要完成光标移动、字符串查找、删除、复制和粘贴等操作。只要按<Esc>键，即可进入命令模式。
 - 输入模式。在命令模式下，输入“i” 键就可以切换到输入模式。该模式中的主要操作就是输入文件内容，可以对文件正文进行修改。
 - 末行模式。在命令模式下，输入“:” 即可进入末行模式，可以保存文件、退出编辑器等，最后一行会出现“:” 提示符。

Vi 编辑器的使用图示



[root@localhost~]# vim 文件名



Vi 编辑器常用快捷键

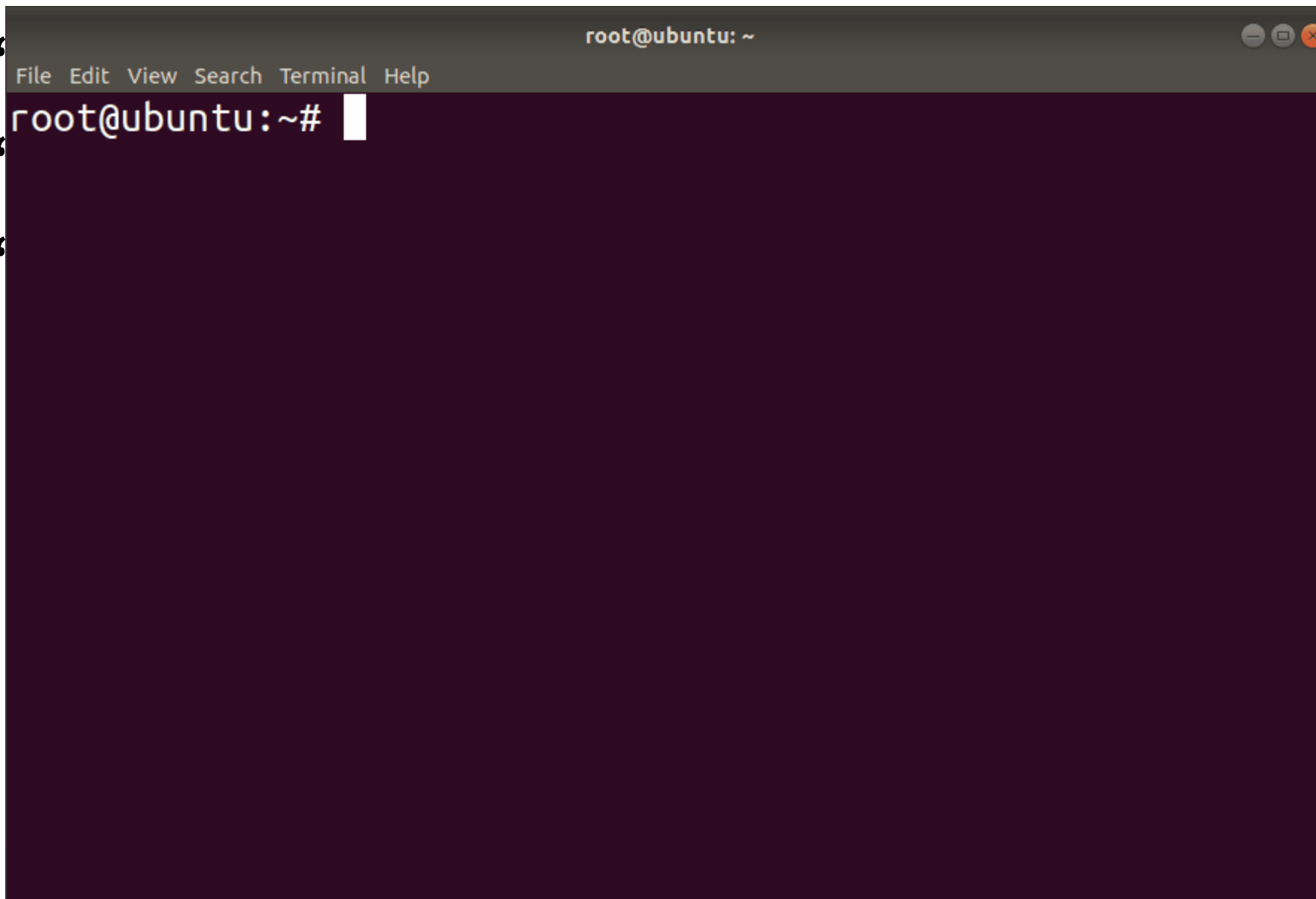


- 使用 “dd” 命令可以删除当前光标所在行
- 使用 “yy” 命令可以复制当前行的内容到剪贴板
- 输入 “p” 可粘贴剪贴板中的内容

Vi 编辑器常用快捷键



- 使用 “
- 使用 “
- 输入 “



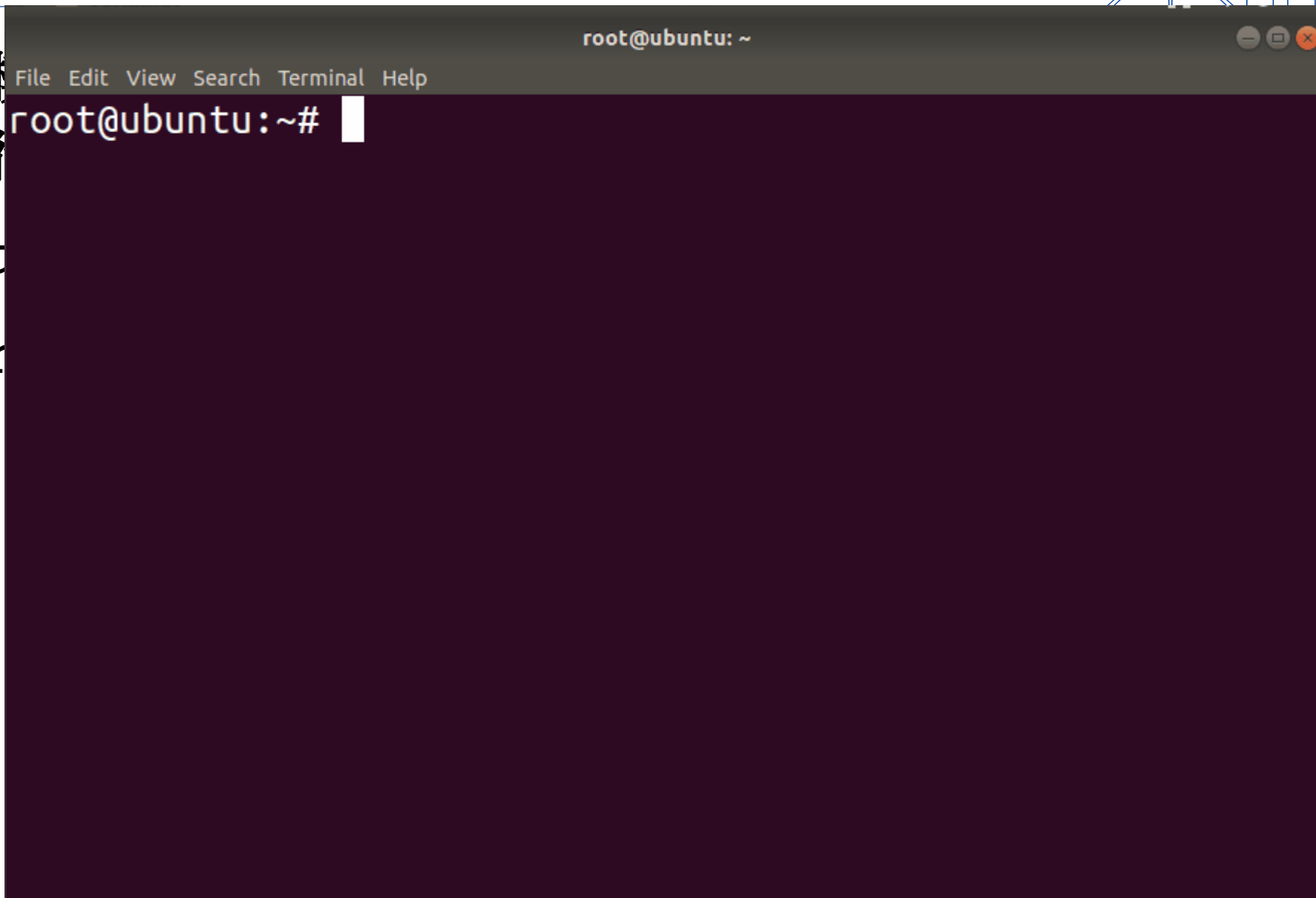
Vim文件内容查找



- 在命令模式下，按</>键后输入指定的字符串，将从当前光标处开始向后进行查找。
- 按<Enter>键后将查找并高亮显示结果。
- 输入“n”移动到下一个查找结果，输入“N”移动到上一个查找结果。

Vim文件内容查找

- 在命令模式下，按`/`，光标向后进行查找。
- 按`<Enter>`，开始查找。
- 输入“`r`”，显示查找结果。



处开始

查找结



信息安全综合实践

Linux的用户和权限管理



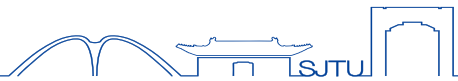
上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

用户和组的概念



- 用户其实就是一种进行认证或授权的标识（ID）。只有通过认证的用户才可以访问相应的资源，而对于同一个资源，不同的用户又具有不同的访问权限。
- 在 Linux 系统中，根据系统管理的需要，将用户账号分为三种不同的类型：超级用户、普通用户和程序用户。每种类型的用户账号所拥有的权限和担任的角色各不相同。

超级用户



- 超级用户： root 是 Linux 系统中默认的超级用户账号，对系统拥有完全权限。
- 使用root 账号，管理员可以突破系统的一切限制，方便地维护系统。
- 由于 root 用户权限太大，因此一般不建议直接用 root 账号登录系统，而是先使用普通用户账号登录，当要进行系统管理维护任务时，才临时转换到 root 身份。

```
root@ubuntu: ~#
```

普通用户和程序用户



- 普通用户账号需要由 root 用户或其他管理员用户创建，拥有的权限受到一定限制，一般只在用户自己的家目录中有完全权限。
- 程序用户最大的特点是不能登录系统，其主要用于让后台进程或服务类进程以非管理员的身份运行。它们大多是在安装系统及部分应用程序时自动添加的，权限一般比较低。

/etc/passwd 是存储用户账户信息的文本文件

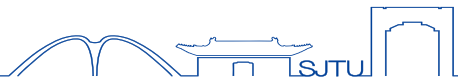


```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

39 gnome-initial-setup:x:120:65534::/run/gnome-initial-setup:/bin/false
40 gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
41 test:x:1000:1000:Ubuntu1804,,,:/home/test:/bin/bash
```

- 第一行就是 root 用户的信息，最后一行是安装系统时所创建的 test 用户的信息。
- 除这两个用户之外，其余的都是程序用户，程序用户用来支撑系统或某些软件运行，不能用它们来登录，在后续内容中不再提及这些程序用户。

UID 和 GID



- **UID** (User Identifier, 用户标识符) 是 Linux 系统中每个用户账号的唯一标识符, 对于Linux 系统来说, UID 是区分用户的基本依据 (类似于 Windows 系统中的 SID)。root 用户的 UID 为固定值 0, 程序用户账号的 UID 默认为 1~999, 1000~60000 的 UID 默认分配给普通用户账号使用。
- 每个用户组有一个数字形式的标识符, 称为 **GID** (Group Identifier, 组标识符)。root组的 GID 为固定值 0, 程序组的 GID 默认为 1~999, 普通组的 GID 默认为 1000~60000。
- 需要注意的是, Linux 系统其实只识别 UID 和 GID, 用户账号和组账号只是为了方便人们记忆而已。例如 root 之所以是超级用户, 并不是因为它的名字叫 root, 而是因为它的 UID 为 0。

利用 id 命令查看用户身份信息



```
root@ubuntu:~# id student
uid=1001(student) gid=1001(student) groups=1001(student)
root@ubuntu:~#
```

```
root@ubuntu:~# id root
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~#
```

- “gid” 部分表示用户所属的基本组，“groups” 部分表示用户所属的基本组和附加组。如果用户没有加入任何附加组，那么在“组”部分就只显示用户的基本组。

/etc/passwd 是存储用户账户信息的文本文件



```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

39 gnome-initial-setup:x:120:65534::/run/gnome-initial-setup:/bin/false
40 gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
41 test:x:1000:1000:Ubuntu1804,,,:/home/test:/bin/bash
```

用户名	密码占位符，以 x标记	UID	GID	用户描述	home目录	shell
-----	----------------	-----	-----	------	--------	-------

test用户名，x 表示加密后的密码存储在 /etc/shadow 文件中

1000 User ID, 1000 Group ID, Ubuntu1804用户描述，/home/test用户的家目录，/bin/bash用户默认的shell(shell可以修改)，程序用户的默认 Shell为/sbin/nologin，意味着不允许登录。

shadow文件（/etc/passwd的影子文件）



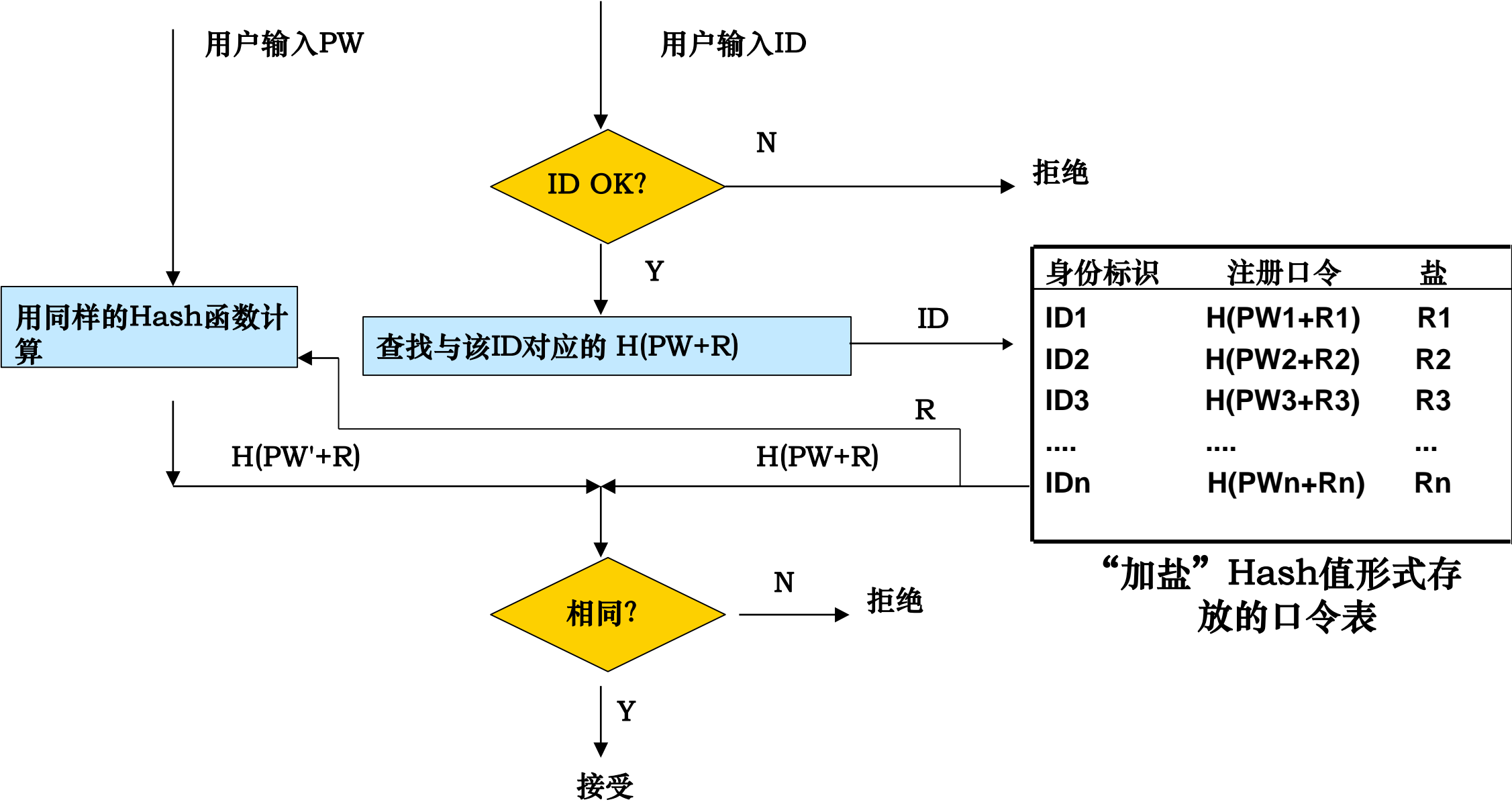
存储用户加密密码的文件，每一行表示一个用户账户的信息。

```
root@ubuntu:/home/test# cat /etc/shadow
root:$6$t5U2pZ2W$F4TPkqK0xNGs9veoJMgc435ZI9050cZsqYg7.f2oE0bRzGPpycto7rX0/oH4fkD9M1XnvOPxbZslQdL0BmGETY/:19594:0:99999:7:::
daemon*:18885:0:99999:7:::
bin*:18885:0:99999:7:::
sys*:18885:0:99999:7:::
sync*:18885:0:99999:7:::
games*:18885:0:99999:7:::
man*:18885:0:99999:7:::
lp*:18885:0:99999:7:::
mail*:18885:0:99999:7:::
hplip*:18885:0:99999:7:::
geoclue*:18885:0:99999:7:::
pulse*:18885:0:99999:7:::
gnome-initial-setup*:18885:0:99999:7:::
gdm*:18885:0:99999:7:::
test:$5$1w06iWlekq0dDhgZ$Ka2UCB/5j66S5yVslbzx0r.RpYYqoeUEw.aBHvWlT9C:19500:0:99999:7:::
```

用户名	加密的密码	密码上次修改的日期	密码过期期限	密码变更周期	密码过期前的警告天数	保留域, 最后两个字段留空, 用于以后的扩展
-----	-------	-----------	--------	--------	------------	------------------------

\$5\$ SHA-256 , 1wO6iWlekq0dDhgZ 随机生成的盐值，后面是经过 SHA-256 哈希处理的密码，基于用户输入的密码和随机盐值计算得出的。当用户尝试登录时，系统会使用输入的密码和盐值，然后通过相同的 SHA-256 哈希函数计算得出哈希值，与存储在 /etc/shadow 文件中的哈希值进行比较，以验证密码的正确性。

加盐Hash口令表



useradd 命令——创建用户账号



useradd student

在 Linux 系统中，useradd 命令在添加用户账号的过程中会自动完成以下几项任务：

- 在“/etc/passwd”文件和“/etc/shadow”文件的末尾增加该用户账号的记录。
- 创建与该用户账号同名的基本组账号
- 在创建用户 student 之后，可以分别查看/etc/passwd、/etc/shadow 文件新增加的信息。

useradd student



```
root@ubuntu:~# useradd student
root@ubuntu:~# tail /etc/passwd
saned:x:114:119::/var/lib/saned:/usr/sbin/nologin
avahi:x:115:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:116:121:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:118:122::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:119:123:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
test:x:1000:1000:Ubuntu1804,,,:/home/test:/bin/bash
student:x:1001:1001::/home/student:/bin/sh
root@ubuntu:~# tail /etc/shadow
saned*:18885:0:99999:7:::
avahi*:18885:0:99999:7:::
colord*:18885:0:99999:7:::
hplip*:18885:0:99999:7:::
geoclue*:18885:0:99999:7:::
pulse*:18885:0:99999:7:::
gnome-initial-setup*:18885:0:99999:7:::
gdm*:18885:0:99999:7:::
test:$5$1w06iWlek9dDhgZ$Ka2UCB/5j66S5yVs1bzxOr.RpYYgoeUEw.aBHvWlT9C:19500:0:99999:7:::
student!:19599:0:99999:7:::
```


passwd 命令——为用户账号设置密码



```
root@ubuntu: ~  
File Edit View Search Terminal Help  
root@ubuntu:~#
```

passwd student



```
root@ubuntu:~# passwd student
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ubuntu:~# tail /etc/shadow
saned:!:18885:0:99999:7:::
avahi:!:18885:0:99999:7:::
colord:!:18885:0:99999:7:::
hplip:!:18885:0:99999:7:::
geoclue:!:18885:0:99999:7:::
pulse:!:18885:0:99999:7:::
gnome-initial-setup:!:18885:0:99999:7:::
gdm:!:18885:0:99999:7:::
test:$5$1w06iWlekg0dDhgZ$Ka2UCB/5j66S5yVslbzx0r.RpYYgoeUEw.aBHvWlT9C:19500:0:99999:7:::
student:$6$mHSSMAgz$T3rK6gNE/VG/vtopzHXJniKm0U0GuvowEUgXX4.puLoKD5Qvz0e1/dzC5rCo8fpBwndKScXc
fDXkY90x3wS0g1:19599:0:99999:7:::
```

如何批量修改密码？



- `echo "username:new_password" | sudo chpasswd`
- 不用重复输入密码确认信息

```
root@ubuntu:~#
```

su 命令 (Switch User) —— 切换用户身份



- 切换到超级用户：如果未指定用户名，su命令会切换到超级用户 (root)

su 或 su -

- 切换到其他用户：可以通过指定用户名来切换到其他用户

su student 或 su - student

非完整切换与完整切换



- 在执行 su 命令时，如果命令之后不加“-”，如“su student”，这种切换方式称为非登录式切换，切换时不会读取目标用户的配置文件，属于非完整切换。
- 如果命令之后加上“-”，如“su - student”，则称这种切换方式为登录式切换，切换时会自动读取目标用户的配置文件，属于完整切换。一般推荐采用登录式切换方式。

```
test@ubuntu: ~  
File Edit View Search Terminal Help  
test@ubuntu:~$
```

```
test@ubuntu: ~  
File Edit View Search Terminal Help  
test@ubuntu:~$
```

使用 sudo 机制提升权限



- sudo (superuser do) 用于以超级用户 (root 用户) 的权限来执行命令。允许授权的用户在需要时以临时的方式获得更高的权限，以便执行需要特权的操作，而无需长时间以管理员身份登录。
- 普通用户使用sudo命令以root身份创建新用户。

```
test@ubuntu:~$ sudo useradd teacher
[sudo] password for test:
test@ubuntu:~$ tail /etc/passwd
avahi:x:115:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:116:121:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:118:122:,:/var/lib/geoclue:/usr/sbin/nologin
pulse:x:119:123:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:120:65534:,:/run/gnome-initial-setup:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
test:x:1000:1000:Ubuntu1804,,,:/home/test:/bin/bash
student:x:1001:1001:,:/home/student:/bin/sh
teacher:x:1002:1002:,:/home/teacher:/bin/sh
```

问题



- 为什么普通用户test可以执行管理员命令？

配置sudo权限



- 要使用 sudo 命令必须先经过管理员的授权设置，需要修改配置文件 “/etc/sudoers”

在sudoers文件中的基本配置格式

用户

主机名列表=命令程序列表

被授权的用户

在哪些主机中使用

允许执行哪些命令

其他用户和组相关命令



- `userdel` 命令——删除用户账号
- `groupadd` 命令——创建用户组
- `gpasswd` 命令——添加、删除组成员
- `groupdel` 命令——删除用户组

Linux的rwx文件权限



每个文件都有三种权限

权限	文 件	目 录
r	查看文件内容	查看目录内容（显示子目录、文件列表）
w	修改文件内容	修改目录内容（在目录中新建、删除文件或子目录）
x	执行该文件（程序或脚本）	执行 cd 命令进入或退出该目录

Linux的rwx文件权限



- ls -al
 - 显示当前目录的详细信息
 - 查看文件的权限信息

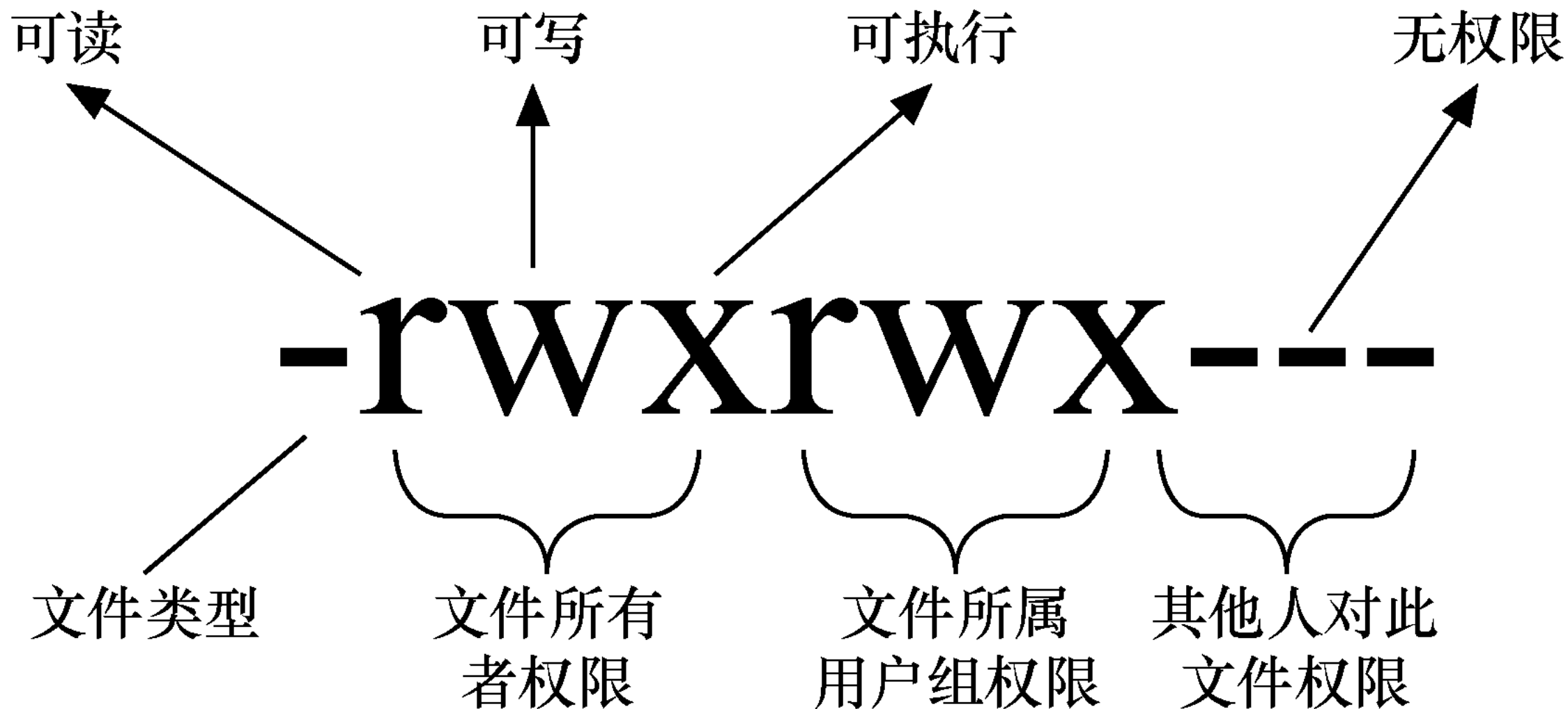
文件类型	属主权限			属组权限			其他用户权限		
0	1	2	3	4	5	6	7	8	9
d	rwx			r-x			r-x		
目录文件	读	写	执行	读	写	执行	读	写	执行

```
total 72
drwx-----  9 root root 4096 Sep  8 07:41 .
drwxr-xr-x 24 root root 4096 Aug 23 08:52 ..
-rw-r--r--  1 root root   18 Sep  8 05:26 1.txt
-rw-----  1 root root 7656 Sep  8 07:41 .bash_history
-rw-r--r--  1 root root 3106 Apr  9 2018 .bashrc
drwx-----  2 root root 4096 Sep 15 2021 .cache
drwx-----  3 root root 4096 Aug 23 22:46 .gnupg
-rw-r--r--  1 root root    8 Sep  8 04:31 jkasldkjfcqerckdafe.txt
drwx-----  2 root root 4096 Aug 30 09:18 .john
-rw-----  1 root root   35 Sep  7 08:53 .lessht
drwxr-xr-x  3 root root 4096 Aug 24 01:13 .local
-rw-r--r--  1 root root  148 Aug 17 2015 .profile
drwxr-xr-x  2 root root 4096 Sep  4 06:36 .rpmdb
drwxr-xr-x  6 root root 4096 May 22 17:33 snap
drwx-----  2 root root 4096 Sep  5 07:22 .ssh
-rw-----  1 root root 7552 Sep  8 07:41 .viminfo
```

-rwxrwx---

- **第一个属性代表这个文件的类型**
 - 为[d]则是目录
 - 为[-]则是文件
 - 为[l]则表示为链接文件(link file)
 - 为[b]则表示为设备文件中可供储存的接口设备
 - 为[c]则表示为设备文件中的串行端口设备，例如键盘、鼠标。

其它的权限位



利用 chmod 命令设置权限



- 通过 chmod (change mode) 命令可以设置更改文件或目录的权限，只有文件所有者或root 用户才有权用 chmod 命令改变文件或目录的访问权限。
- 在用 chmod 命令设置权限时，可以采用两种不同的权限表示方法：字符形式和数字形式。

数字形式的 chmod 命令



- r、w、x 权限字符可以分别表示为八进制数字 4、2、1
- 表示一个权限组合时需要将数字进行累加，例如，“rwx”采用累加数字形式表示成“7”，“r-x”采用累加数字形式表示成“5”
- “rwxr-xr-x”由3组权限组成，因此可以表示成“755”，“rw-r--r--”可以表示成“644”
- 对应二进制数，例如rwx = 111、r-x = 101、r-- = 100

权限项	读	写	执行	读	写	执行	读	写	执行
字符表示	r	w	x	r	w	x	r	w	x
数字表示	4	2	1	4	2	1	4	2	1
权限分配	文件所有者			文件所属组			其他用户		

举例



例如，对/tmp/test 目录进行如下权限设置：

- 所有者具有读、写和执行权限。
- 所属组具有读和执行权限。
- 其他用户具有读和执行权限。

```
root@ubuntu:~# chmod 755 /tmp/test
root@ubuntu:~# ls -l -d /tmp/test
drwxr-xr-x 2 root root 4096 Sep  8 09:35 /tmp/test
root@ubuntu:~# ll -d /tmp/test
drwxr-xr-x 2 root root 4096 Sep  8 09:35 /tmp/test/
```

打开所有权限



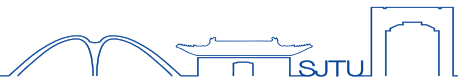
```
root@ubuntu:~# chmod 777 /tmp/test
root@ubuntu:~# ll -d /tmp/test
drwxrwxrwx 2 root root 4096 Sep  8 09:35 /tmp/test/
```

练习



1. 你希望一个文件对所有用户都是只读的，你应该使用哪个chmod数字命令？
2. 你想让一个文件对所有者是可读、可写、可执行，而对组和其他用户是只读的，你应该使用哪个chmod数字命令？
3. 你有一个文件，其当前权限是755。你希望移除其他用户的所有权限，你应该使用哪个chmod数字命令？
4. 一个文件的权限被设置为731，请描述所有者、组和其他用户的权限。

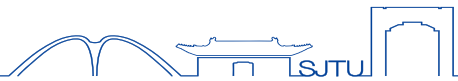
练习答案



1. 你希望一个文件对所有用户都是只读的，你应该使用哪个chmod数字命令？ **chmod 444 文件名**
2. 你想让一个文件对所有者是可读、可写、可执行，而对组和其他用户是只读的，你应该使用哪个chmod数字命令？
chmod 744 文件名
3. 你有一个文件，其当前权限是755。你希望移除其他用户的所有权限，你应该使用哪个chmod数字命令？ **chmod 750 文件名**
4. 一个文件的权限被设置为731，请描述所有者、组和其他用户的权限。

所有者：读、写、执行； 组：写、执行； 其他用户：执行

练习



在Linux系统中，下列哪项内容不包含在/etc/passwd文件中？

A. 用户登录后使用的SHELL

B. 用户口令

C. 用户主目录

D. 用户名

答案



在Linux系统中，下列哪项内容不包含在/etc/passwd文件中？

A. 用户登录后使用的SHELL

B. 用户口令

C. 用户主目录

D. 用户名

存储在/etc/shadow文件中，只有root用户可以访问。

Linux的日志功能



- Linux系统拥有强大而灵活的日志功能，可以保存几乎所有的操作记录。
- Linux 可以编写脚本对日志进行检索，并基于它们的内容去自动执行某些功能。
- Linux 日志默认存储在 `/var/log` 目录中。
- 大多数日志只有root账户才可以读。

Linux的日志文件



- `/var/log/secure`
 - Linux系统安全日志，记录用户和工作组变化情况、用户登录认证情况、网络连接信息等。
 - Ubuntu 和 Debian 在 `/var/log/auth.log` 中存储认证信息，而 RedHat 和 CentOS 则在 `/var/log/secure` 中存储该信息。
- `/var/log/kern.log`
 - 记录内核产生的日志。

Linux的日志文件



- 用户登录相关日志

- /var/log/wtmp
 - 记录每个用户登录、注销及系统的启动、停机的事件
- /var/run/utmp
 - 记录当前登录的每个用户
- /var/log/lastlog
 - 记录最近成功的登录和最后一次不成功的登录

Linux的日志文件



- `/var/log/faillog`
 - 记录用户登录失败信息。错误登录命令也会记录在本文件中。
- `/var/log/maillog`
 - 记录了每一个发送到系统或从系统发出的电子邮件的活动。
 - 可以用来查看用户使用哪个系统发送工具或把数据发送到哪个系统。

Linux安全性高于windows?



系统设计Linus Torvalds

- **性能和可靠性更重要**，任何系统的安全都不可能完美，必须与其它优先事项权衡利弊。
- “那些将安全置于一切之上的人都疯了，安全本身是没有意义的，问题总是会出现在某个地方，安全从来不是需要你真正关注的东西。”



Linux内核缺陷



- 2004年暴露出20多个安全漏洞
- 2009年，黑客公开了可以攻击所有新旧Linux系统的一个漏洞，可以通过此漏洞使用空指针获得root权限，即使开启了SELinux也于事无补。
- 2016年，发现在Linux内核密钥管理和保存功能中存在一个高危的提权0day漏洞，影响当时超过66%的安卓手机和1000万Linux PC和服务端
- 2017年，发现Linux内核IPSEC框架中的一个内存越界漏洞
- 2017年，发现Linux内核存在四个极度危险的漏洞—代号“Phoenix Talon”，影响几乎所有Linux kernel 2.5.69 - Linux kernel 4.11的内核版本
-

不安全的Linux服务



- 不安全的服务：rlogin, rsh, telnet等
- 家用和小型办公室路由器中，有很多都装的是过时Linux内核固件。



信息安全综合实践

Windows安全基础



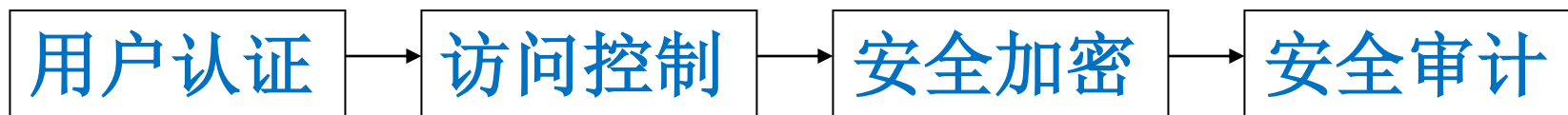
上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

本节内容



- Windows安全机制

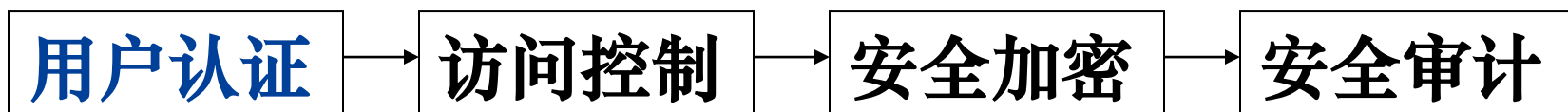
- 用户认证
- 访问控制
- 安全保密
- 安全审计



文件/文件系统
加密

审计/日志机制

用户认证



Windows系统内置用户和组



内置用户：

- **Administrator**：这是系统的超级用户，具有完全的系统访问权限。默认情况下，系统安装后会创建一个 Administrator 用户。该用户可以对系统进行任何更改。
- **Guest**：临时访客账户。Guest用户通常受到限制，拥有较低的权限。

内置组：

- **Administrators**：管理员组。该组拥有对系统的完全访问权限，可以对系统进行所有操作。
- **Users**：拥有一般的操作权限，不能进行敏感操作。
- **Guests**：具有有限的权限，通常只能访问系统上的一些共享资源。

net user命令



命令提示符是Windows系统中的命令行工具，用于管理用户账户。允许管理员在命令行界面上执行各种用户账户操作，如创建用户、修改密码等。

- `net user administrator` 显示administrator用户的信息
- `net user student 123456 /add` 添加用户名为student，密码为123456的用户账户
- `net user student /del` 将student用户删除

```
C:\Documents and Settings\test>net user student1 /del  
命令成功完成。
```

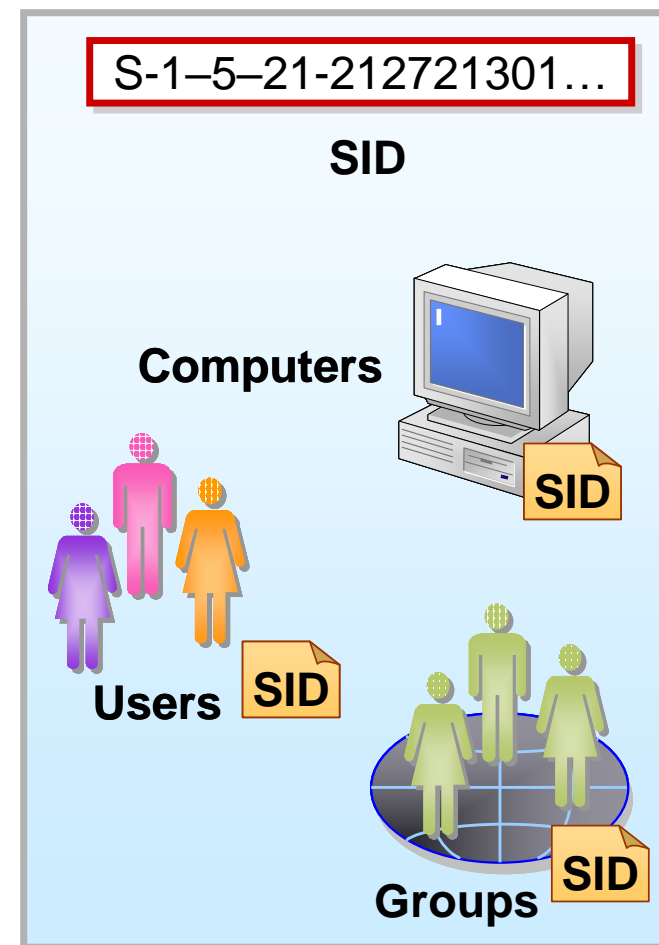
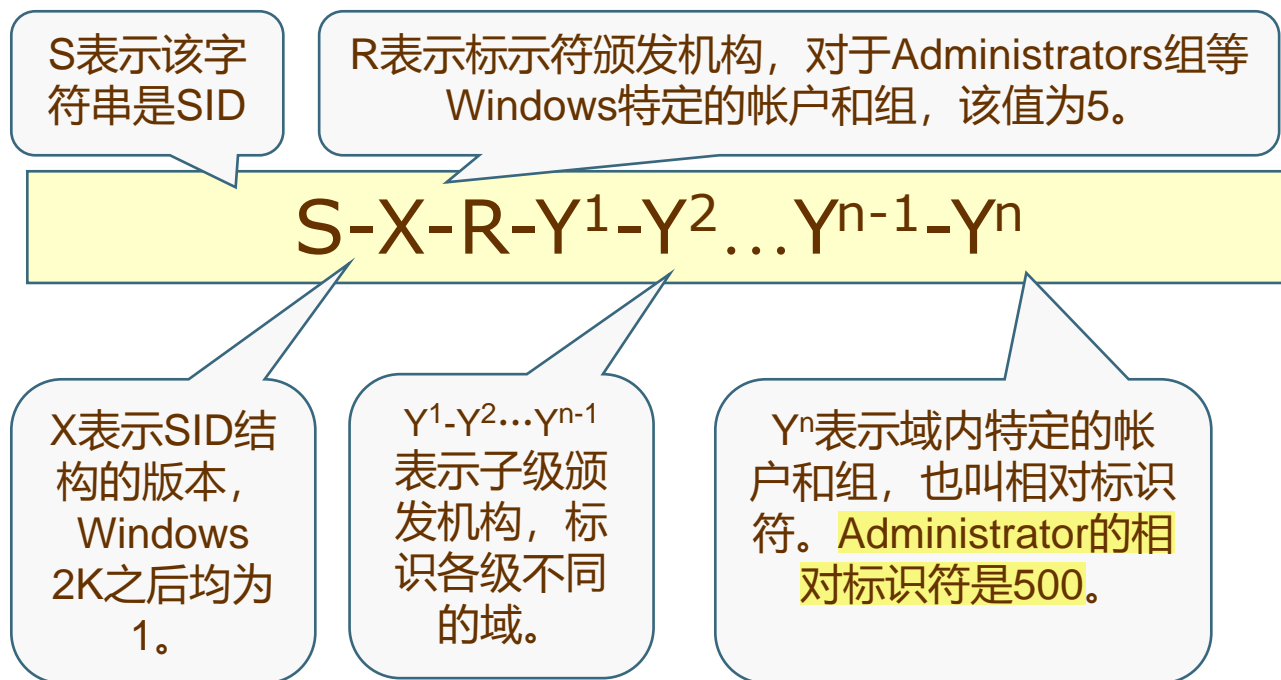
```
C:\Documents and Settings\test>net user student2 /del  
命令成功完成。
```

安全标识符



Security Identifiers, SID

S-1-5-21-515967899-630328440-725345543-500



练习



下面哪个是administrator用户的SID?

A.S-1-5-21-3698344474-843673033-3679835876-100

B.S-1-5-21-3698344474-843673033-3679835876-500

C.S-1-5-21-3698344474-843673033-3679835876-1000

D.S-1-5-21-3698344474-843673033-3679835876-1001

练习答案



下面哪个是administrator用户的SID?

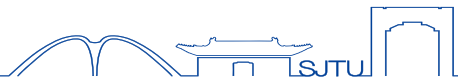
A.S-1-5-21-3698344474-843673033-3679835876-100

B.S-1-5-21-3698344474-843673033-3679835876-500

C.S-1-5-21-3698344474-843673033-3679835876-1000

D.S-1-5-21-3698344474-843673033-3679835876-1001

SAM文件



- SAM (Security Accounts Manager)
 - 所有本地帐号的登录名和口令等相关信息都保存在这个文件中。
 - 系统对保存在SAM中的口令信息进行了加密处理，以保护口令信息的机密性。
 - LAN Manager散列算法 (LM)
 - NT散列算法 (NTLM/NTLMv2)
- 在系统运行期间， SAM文件被system账号锁定，即使是administrator账号也无法对其进行删除等操作。
- SAM文件存放的位置
 - C:\Windows\System32\config (本机打开查看)

LM哈希和NT哈希



- Windows操作系统中用于存储用户密码的两种不同的密码哈希算法。
- LM哈希是早期Windows操作系统中使用的密码哈希算法，主要出现在Windows NT之前的版本中。
- NT哈希是Windows NT以及后续版本中使用的密码哈希算法，用于替代LM哈希。
- Win7之前的系统中同时采用这两种方式存储密码，之后的系统不采用LM哈希。

User	RID	LM-Password	NT-Password	LM-Hash	NT-Hash	Description
<input checked="" type="checkbox"/> Administrator	500	???????	???????	78C7649CD439B9F9A...	75D276BB172E352BE...	
<input type="checkbox"/> Guest	501	<Disabled>	<Disabled>	000000000000000000...	000000000000000000...	
<input checked="" type="checkbox"/> HelpAssistant	1000	????????????????	????????????????	A31E3992865C3A0C...	FD026B5C854CB8861...	
<input checked="" type="checkbox"/> SUPPORT_388945a0	1002	<Disabled>	????????????????	000000000000000000...	CED3AD45055295F3B...	

练习



以下Windows的哪个版本可以得到LM hash?

A.Windows XP

B.Windows Vista

C.Windows 7

D.Windows server 2008

练习答案



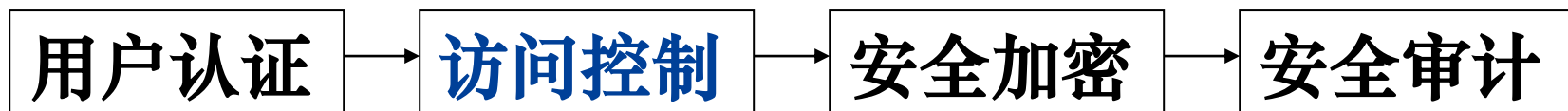
以下Windows的哪个版本可以得到LM hash?

A.Windows XP

B.Windows Vista

C.Windows 7

D.Windows server 2008



Windows的访问控制过程



安全主体的访问令牌→客体的安全描述

1. 用户登录时，系统为其创建访问令牌。
2. 用户启动程序时，线程获取令牌的拷贝。
3. 程序请求访问客体时，提交令牌。
4. 系统使用该令牌与客体的安全描述进行比较来执行访问检查和控制。



访问令牌



- 访问令牌(Access Token)
 - 主体所有
 - 与特定的Windows账户关联
 - 是用户在通过验证的时候由登陆进程所提供的，所以改变用户的权限需要注销后重新登陆，重新获取访问令牌。

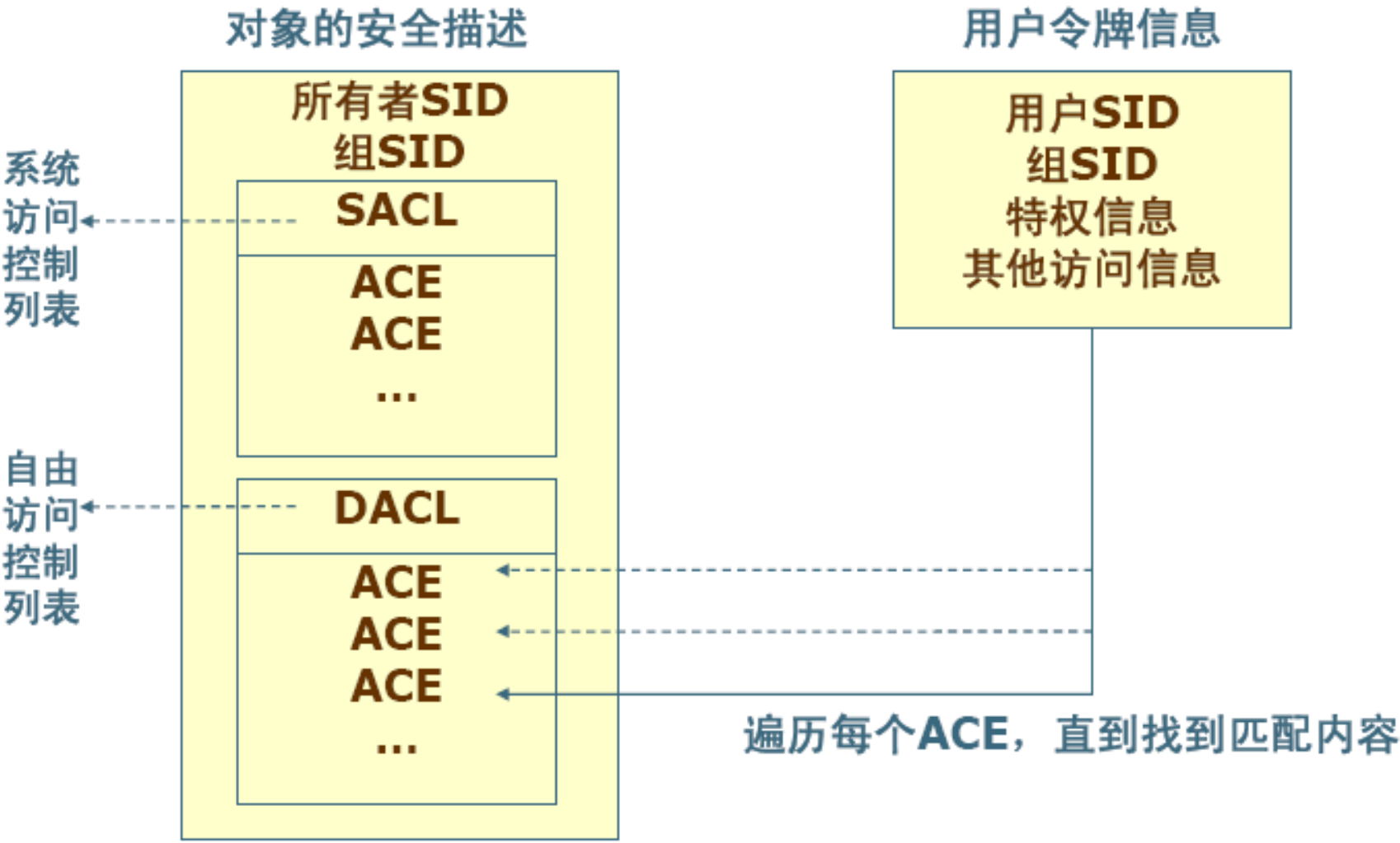
用户令牌信息

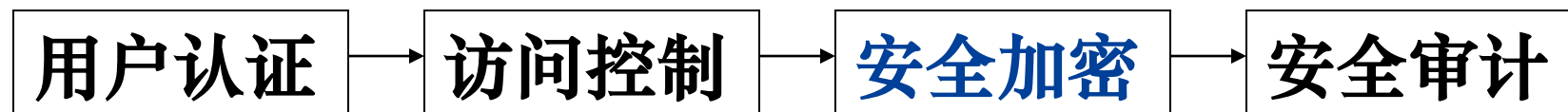
用户SID
组SID
特权信息
其他访问信息

访问对象的安全描述符



- 安全描述符(Security Descriptor)
 - 与客体相关
 - 包括所有者SID和组SID
- 访问控制列表(ACL)
 - 创建对象时也会创建
 - SACL (系统访问方式 (如, 读、写、删除、执行))
 - DACL (自由访问控制列表)





加密文件系统EFS



- Encrypting File System, Windows 核心态
- 位于Windows 核心态，属于 NTFS文件系统。加密和解密动作都在操作系统内核中完成。
- EFS使用密钥加密，不易被破解。以公钥加密，使用公钥对该密钥进行加密。自动备份证书和密钥。
- 可以控制哪些人有权解密或恢复数据。如果用户没有访问计算机的数据存储器，也无法读取加密文件。



Bitlocker



■ Bitlocker

- 在Windows Vista首次引入
- 是一种全卷加密技术，摆脱因电脑硬件丢失构成的威胁
- 同时支持FAT和NTFS两种格式，可以加密可移动的**便携存储设备**，如U盘和移动硬盘
- 有两种工作模式：TPM模式和U盘模式
- “控制面板” - “系统和安全” - “BitLocker 加密”。

BitLocker 驱动器加密

通过使用 BitLocker 保护驱动器，可帮助保护你的文件和文件夹免受未经授权的访问。

操作系统驱动器

C: BitLocker 已关闭



 启用 BitLocker

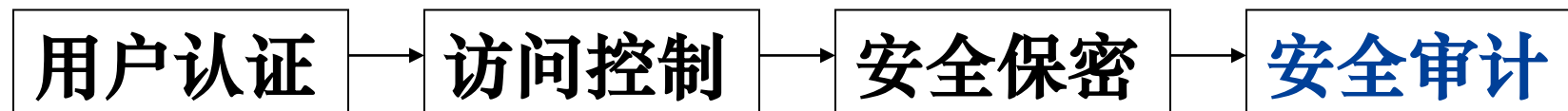
固定数据驱动器

机械硬盘 (D:) BitLocker 已关闭

E (E:) BitLocker 已关闭

可移动数据驱动器 - BitLocker To Go

插入可移动 U 盘以使用 BitLocker To Go。

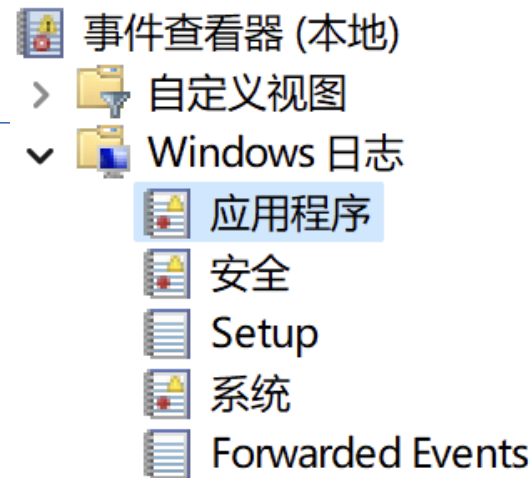


Windows审核机制



- Windows允许用户监视与安全性相关的事件（如失败的登录尝试），因此，可以检测到攻击者和试图危害系统数据的事件。
- 审核策略：即需要记录哪些事件。
- Windows中，**日志文件的类型比较多**。有经验的管理员可通过分析日志来确定入侵者的IP地址以及入侵时间。

Windows 日志



- Windows 日志：
 - 应用程序日志
跟踪应用程序关联的事件。
 - 安全日志
跟踪事件如登录上网、下网、改变访问权限以及系统启动和关闭。
 - 系统日志
跟踪各种各样的系统事件，比如跟踪系统启动过程中的事件或者硬件和控制器的故障。
 - DNS服务器日志、FTP日志、WWW日志跟踪各种各样的系统事件，比如跟踪系统启动过程中的事件或者硬件和控制器的故障。



信息安全综合实践

密码破解实验



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

利用john工具破解Linux密码



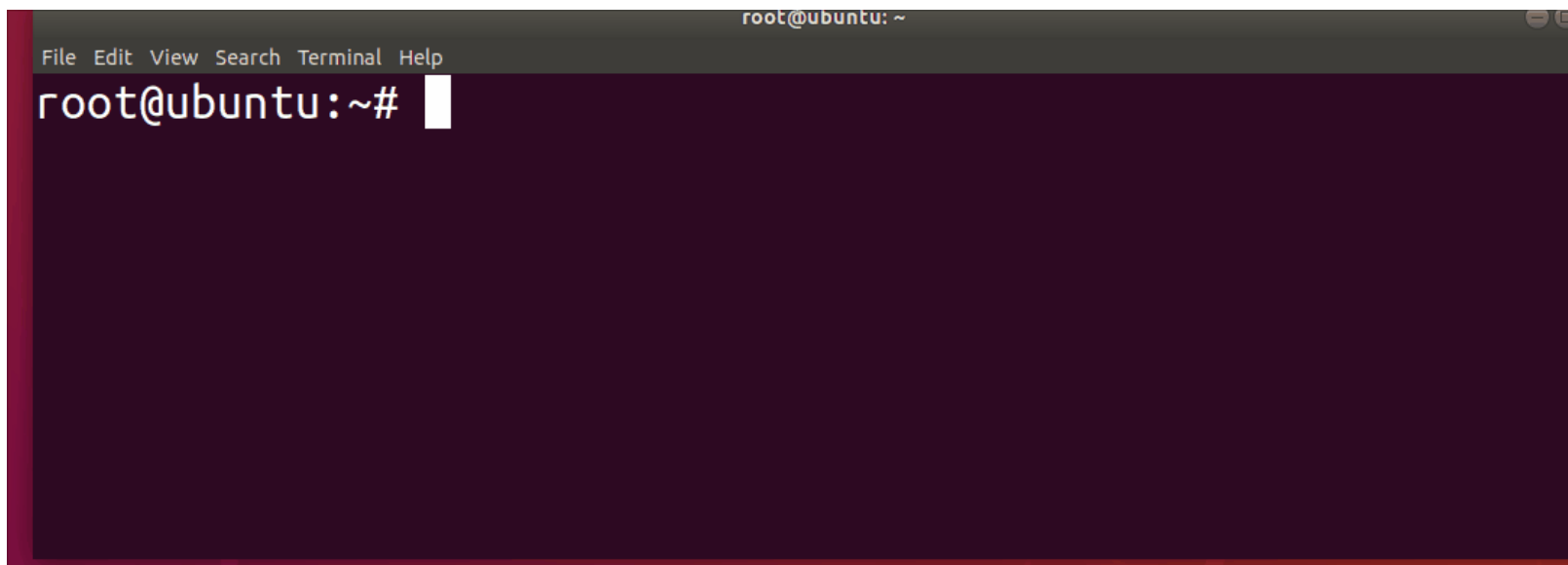
- John the Ripper (通常称为 John) 是一个强大的密码破解工具，支持多种加密算法和攻击模式。

(1)安装 John the Ripper:

- `sudo apt-get update`
- `sudo apt-get install john`

(2)使用John the Ripper进行破解

- `john /etc/shadow`
- `john --show /etc/shadow`



利用SAMInside工具破解Windows密码



```
D:\PwDump>PwDump.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es
```

点击运行桌面的SAMInside工具，通过File-Import from PWDUMP file导入sam2.txt，可以看到一些帐号的弱密码已经自动破解出来了

SAMInside						
File Edit View Tools Audit Service ?						
User	RID	LM-Password	NT-Password	LM-Hash	NT-Hash	Description
<input checked="" type="checkbox"/> Administrator	500	???????	???????	78C7649CD439B9F9A...	75D276BB172E352BE...	
<input type="checkbox"/> Guest	501	<Disabled>	<Disabled>	000000000000000000...	000000000000000000...	
<input checked="" type="checkbox"/> HelpAssistant	1000	???????????????	???????????????	A31E3992865C3A0C...	FD026B5C854CB8861...	
<input checked="" type="checkbox"/> SUPPORT_388945a0	1002	<Disabled>	???????????????	000000000000000000...	CED3AD45055295F3B...	
<input type="checkbox"/> test	1003	TEST	test	01FC5A6BE7BC6929A...	0CB6948805F797BF2...	
<input type="checkbox"/> student	1004	1234	1234	B757BF5C0D87772FA...	7CE21F17C0AEE7FB9...	
<input type="checkbox"/> teacher	1005	5678	5678	A7F94BDC54C75446...	4D3BD16C0B87D0FE...	



信息安全综合实践

课堂练习



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

练习



Linux系统中唯一标识每一个用户的是：

A.UID

B.GID

C.UID和用户名

D.用户名

练习



普通用户test希望使用su命令切换为student用户身份，需要提供____用户的密码？ test命令想执行sudo命令，需要输入____用户的密码？

- A. root
- B. test
- C. student
- D. 不需要密码

练习



在Unix系统中，关于shadow文件说法正确的是？（多选题）

- A、只有超级用户可以查看
- B、保存了用户的密码
- C、增强了系统的安全性
- D、对普通用户是只读的

练习答案



在Unix系统中，关于shadow文件说法正确的是？（多选题）

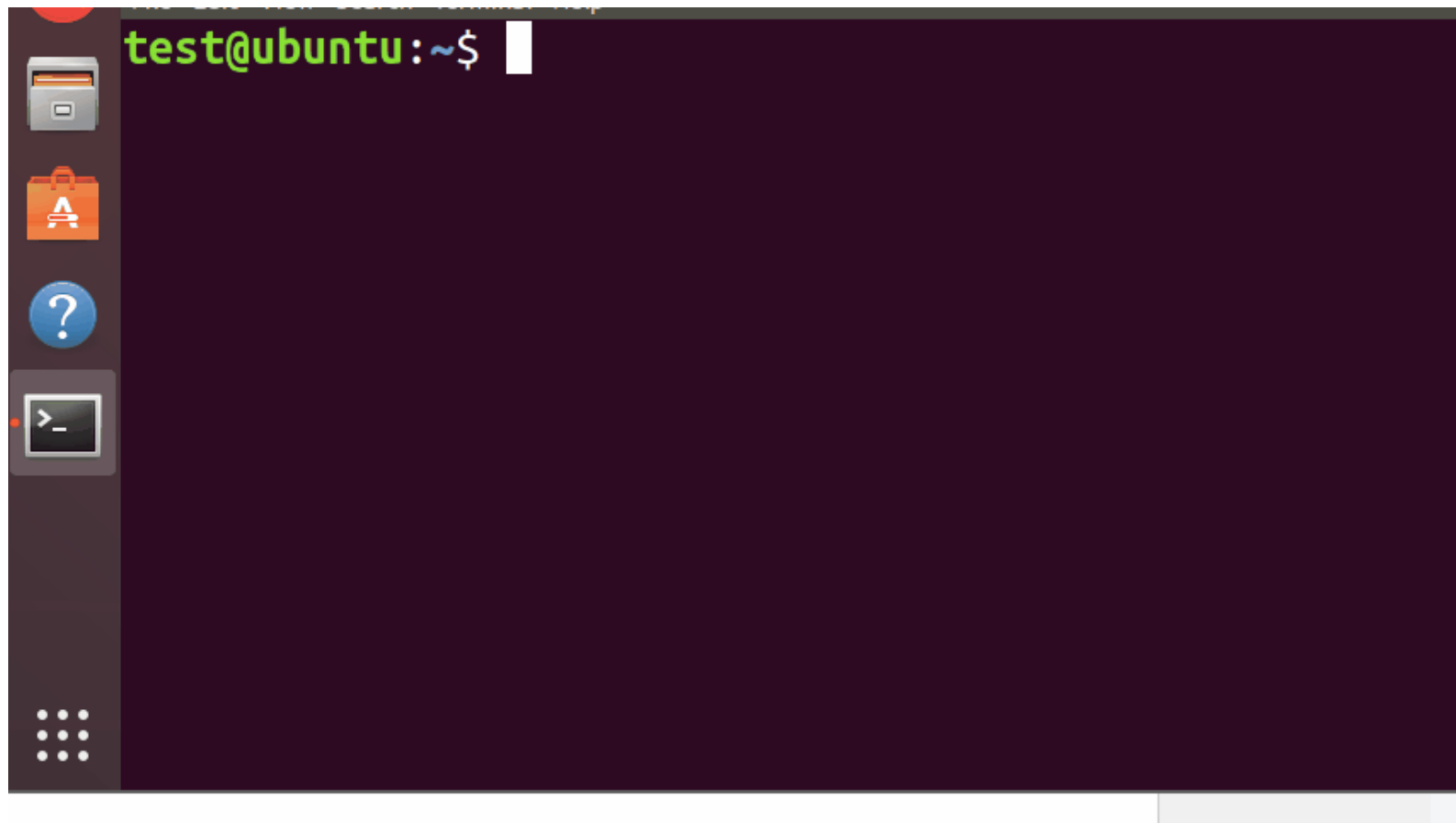
- A、只有超级用户可以查看
- B、保存了用户的密码
- C、增强了系统的安全性
- D、对普通用户是只读的

```
test@ubuntu:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

Linux基础命令补充



- 开启Ubuntu虚拟机终端shell，进入su模式
- `sudo passwd root`
- `su -`



ls命令



- `ls -a` #显示所有文件，包含隐藏文件
- `ls -al` #长列表显示详细信息
- `ls -ld` #显示目录的信息
- `ls -alh` #human readable显示信息

```
root@ubuntu:~#
```

file命令



```
root@ubuntu:~#
```

clear命令



- 清屏

```
root@ubuntu:~# file 1.txt
1.txt: ASCII text
root@ubuntu:~# file /bin/bash
/bin/bash: ELF 64-bit LSB shared object, x86-64, ve
rsion 1 (SYSV), dynamically linked, interpreter /li
b64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, Buil
dID[sha1]=6386b644ab2d987986aeb40325a787a035a4f0d8,
stripped
root@ubuntu:~# █
```

head tail



- **head /etc/passwd** #查看文件头部, **tail /etc/passwd** #查看文件尾部。

```
root@ubuntu:~#
```


wc命令 (word count)



- `wc -l /etc/passwd` #统计/etc/passwd文件行数 (用户数)

```
root@ubuntu:~# wc -l /etc/passwd
```

du命令、df命令



- `du -h /etc/passwd` #查看文件占用空间, `-h`: `--human-readable`
- `df -h` #检查文件系统的磁盘空间占用情况, `-h`, `--human-readable`

```
root@ubuntu:~#
```

grep命令（查找内容）



- `grep "root" /etc/passwd` #在/etc/passwd中查找root
- `grep -n "root" /etc/passwd` #显示行号
- `grep -v "root" /etc/passwd` #反转显示（不包含root）

```
root@ubuntu:~#
```

history (查看历史命令)



- `history` #查看历史命令
- `!5` #把第5条命令重新执行一遍

```
root@ubuntu:~#
```

man命令、--help查看手册



```
root@ubuntu:~#
```

ps命令



- `ps` #显示当前终端当前用户的进程信息
- `ps a` #显示所有终端的进程信息
- `ps aux` #显示所有进程信息

```
root@ubuntu:~#
```

top命令



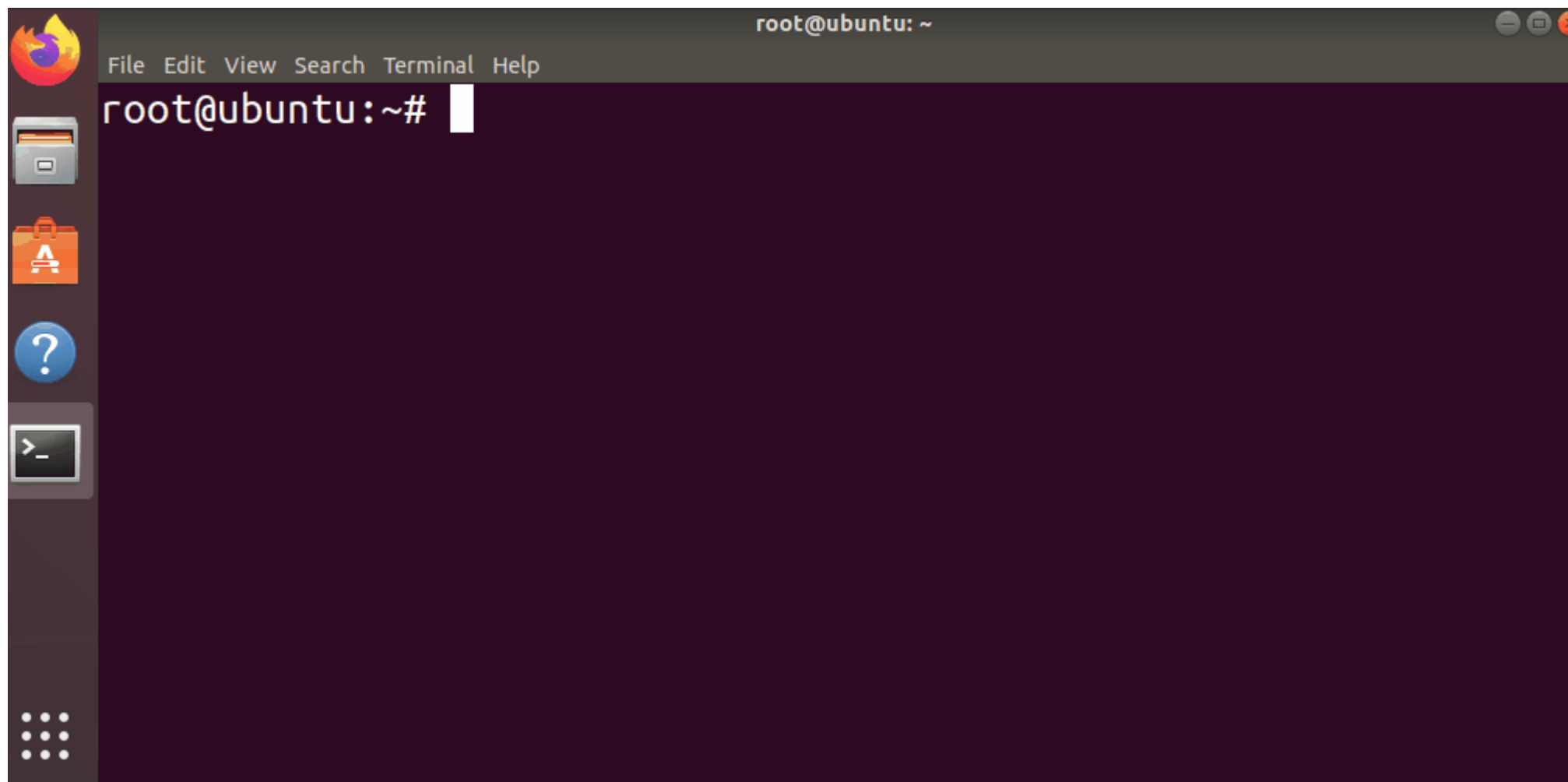
- 实时动态显示系统中各个进程的资源占用情况，默认5秒更新一次

```
root@ubuntu:~#
```

w命令



- w #显示系统中当前登录用户的信息



netstat命令



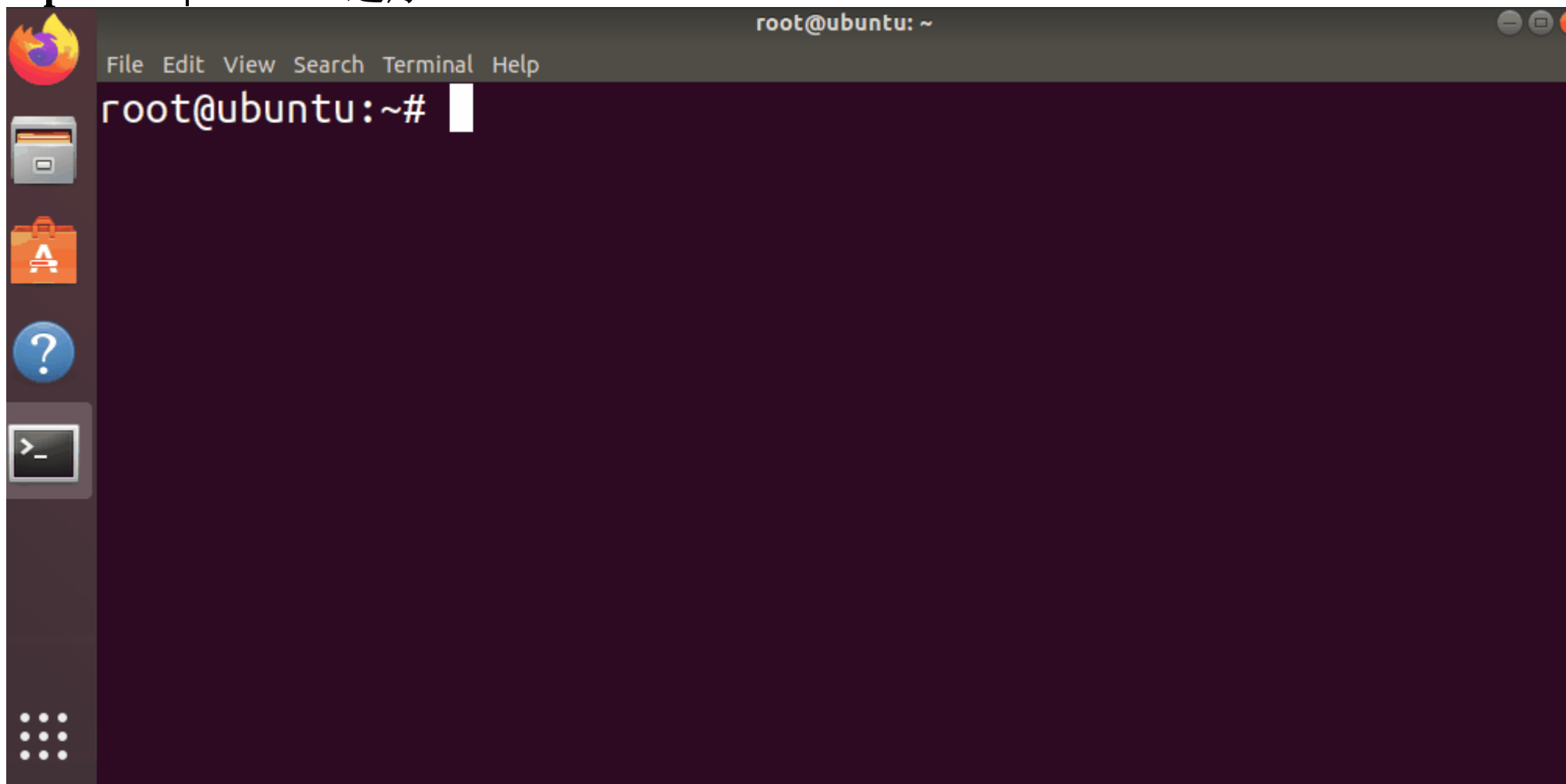
- `netstat -antp` 显示网络状态信息

```
root@ubuntu:~#
```

sort命令



- `cat /etc/passwd | sort` #对输出结果排序
- `cat /etc/passwd | sort -r` #逆序



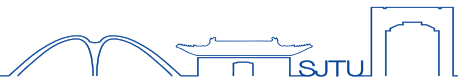
nl命令



- `cat /etc/passwd | sort | nl` #显示行号

```
root@ubuntu:~#
```

思考题



1. Linux 发行版目前主要分为哪几个阵营？简述它们各自的主要特点。
2. Ubuntu中root用户默认使用的是什么 Shell？root的 Shell 命令提示符为 “root@ubuntu:~#”，指出命令提示符中各部分的具体含义。
3. 分别说明根目录下常见的子目录/root、 /etc、 /dev、 /var、 /home、 /bin 和/sbin 的作用。
4. 将工作目录切换到当前用户的家目录。
5. “-” “d” “l” “c” “b” 分别代表的是哪种类别的文件？
6. 以长格式显示/bin/bash文件的详细信息。
7. 查看文件/etc/passwd 的内容，并显示行号。
8. 分别用 more、 less 命令分屏查看/etc/passwd 文件的内容。
9. 在/etc/passwd 文件中查找包含 “root” 字符串的行。
10. 查看 grep 命令的帮助手册。