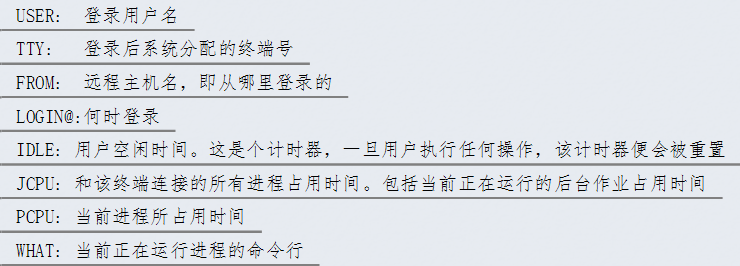
# 查询用户与用户组

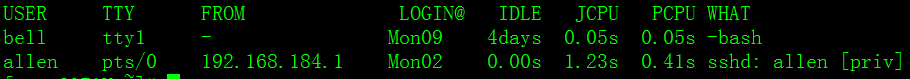
## 1.w命令 查看登录用户以及他们在干什么

1. 表示的内容如下



1. 这个命令用来查看谁登录了系统，以何种方式登录，当前正在干什么
2. 第一个参数表示当前系统时间，up num 表示系统从开机到现在运行了多长时间，这里是7h47min，第三个表示当前登录用户数； 第四个表示系统分别在0.1,0.5,1s中的平均负载。

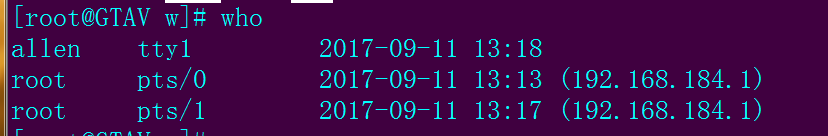
|  |  |
| --- | --- |
| 16:48:27 | 当前系统时间 |
| Up 7:47 | 系统从开机到现在的运行之间 |
| 2 users | 当前登录系统的用户数 |
| Load average:0.00, 0.00, 0,00 | 表示系统在1min,5min,15min的繁忙程度 |



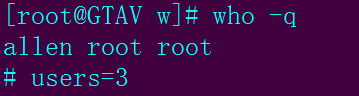
1. 第二列表示用户登录的方式，tty表示从终端登录，pts/num表示从远程登录；what表示当前正在使用的进程，Allen后面还加了一个[priv]，当前正在运行sshd远程客户端管理工具；

## 2.Who命令，统计在线人数

1. 这个命令用来显示谁目前登录了系统，并提供登录系统的时间和ip地址，如下图所示



-q统计登录的总人数



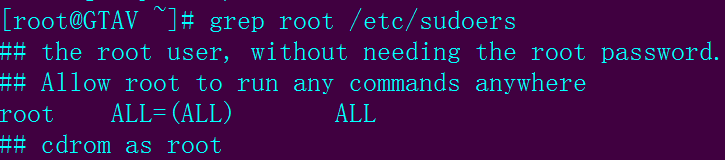
使用功能who –m参数只显示当前登录用户，相当于who am i

## 3.Su 切换用户身份

1. 这个命令用来使用另一个用户身份来执行文件；在Linux中，经常会遇到的问题是一个普通用户在安装，删除程序时权限不够，就需要暂时赋予它高级权限，有两种方式，第一种就是使用su，它可以暂时切换用户身份到root中，从root中切换到普通用户身份不需要密码。不过这种方式的缺陷就是root密码会被人知道；所以这种方式不被推荐，因为它会让管理员密码泄露
   1. –l /- 这个参数用来变更切换用户的shell和home，如果不带参数执行切换，则不会改变当前用户的shell和home；使用这个参数，可以更新切换用户的pyth，shell，和home

## 4.Sudo命令 以另一个用户身份执行命令

第二种方法，让某个普通用户暂时拥有超级权限，不需要知道root密码，只需要管理员把他加到sudoer列表中即可；这种情况下会有一个致命的漏洞，使用“sudo su - root”就可以立即以root执行，而且不需要管理员密码，所以，解决方法看红色部分



|  |  |
| --- | --- |
| Root | 表示当前用户名 |
| ALL | 表示用户的地址，all表示所有网段；也可以是192.168.1.10/24; localhost 表示本地机器 |
| (ALL) | 表示以谁的身份执行，root表示管理员 |
| ALL | 要执行的命令，这里的命令使用命令所在的路径；使用which来查看某个命令所在的路径 |



所以，只要在root这一行的后面，添加上所需要的用户即可；

比如：

它表示nick可以在此网段内使用root命令执行useradd命令；

使用的时候要用如下格式： sudo nick useradd …..

如果单纯使用nick，则依然无法使用Useradd命令，因为必须要有sudo来确保他有权限；

如果要添加多个命令，命令路径之间用逗号隔开

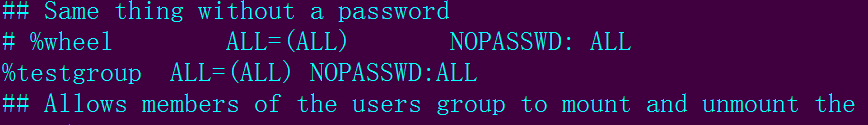


只要在all后面加上nopasswd,就不用在使用sudo时依然要输入密码了；

默认用户会在五分钟后过期，可以修改相关配置来改变这个属性；

Sudo su – 表示切换到root ,”sudo su – root ” 这条命令是禁忌，因为这会让普通用户不需要密码就可以获取管理员的权限，所以，这条命令必须禁止；所以，“bin/su”这条命令绝对不能添加到普通用户可执行命令中

在root会话中，使用visudo可以直接编辑/etc/sudoers文件，和vi类似；下图展示了如何添加一个组到sudo中



这里添加了一个testgroup组到sudo中；不需要密码登录；

<http://man.linuxde.net/sudo> 这篇博客讲解了sudo命令的详细信息；

## 5.Id 查询用户

1. 打印特定用户的gid或者uid，不使用任何参数，则打印当前用户的相关信息；
   1. –G 打印用户所属组的gid
   2. –g 打印有效id

## 6.Groups 查询用户组

1. 这个命令用来查看某个用户所属的组
   1. Groups username 打印用户所属的所有组；

## 7.Finger 用户的查询信息

1. 这个程序用来查看用户的相关信息，它和w类似
   1. Finger 不带任何参数，打印当前登录的所有用户的信息；
   2. Finger username 打印某个用户的登录信息

## 8.Pwck 验证/etc/passwd和/etc/shadow的完整性

1. 默认不带参数，会验证/etc/passwd文件；按照某个固定的格式来验证；

## 9.Grpck 验证/etc/group和/etc/gshadow的完整性

1. 如果验证完整，则不输出任何值，否则输出错误值；

