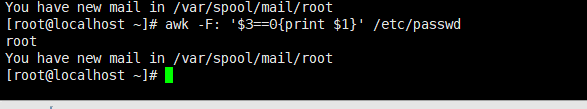
# 1.查看用户信息

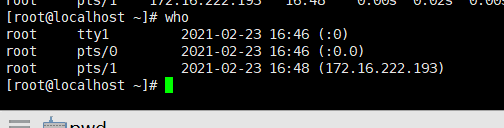
/etc/passwd 查看用户信息文件

/etc/shadow 查看影子文件

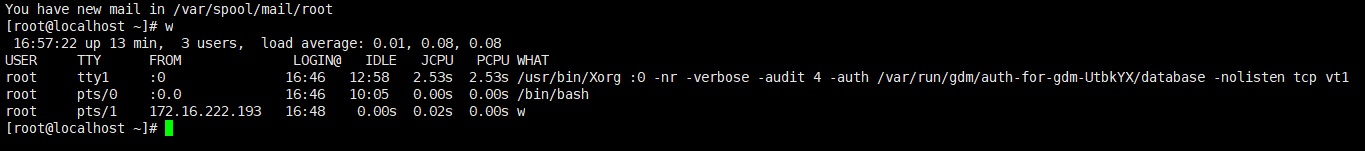
awk -F: '$3==0{print $1}' /etc/passwd （查看系统是否还存在其他的特权账户，uid为0，默认系统只存在root一个特权账户）



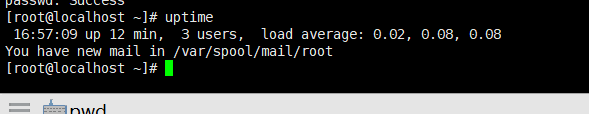
who 查看当前登录用户（tty 本地登陆 pts 远程登录）



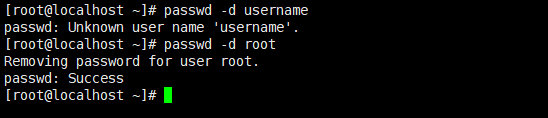
w 查看系统信息，想知道某一时刻用户的行为



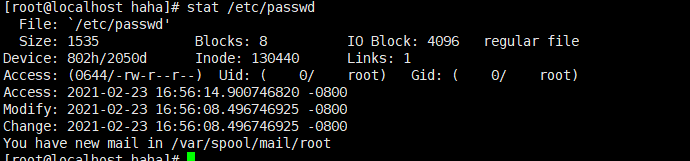
uptime 查看登陆多久、多少用户，负载



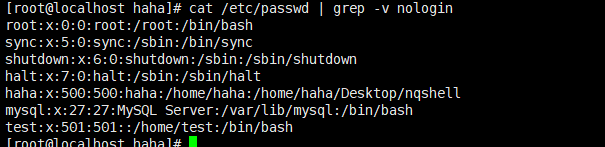
passwd -d username 检查用户是否存在空口令



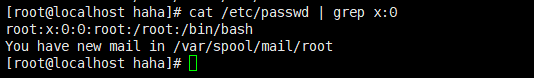
stat /etc/passwd #查看密码文件上一次修改的时间，如果最近被修改过，那就可能存在问题。



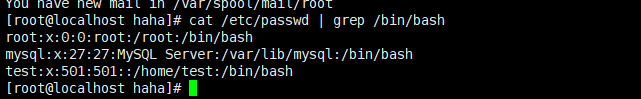
cat /etc/passwd | grep -v nologin #查看除了不可登录以外的用户都有哪些，有没有新增的



cat /etc/passwd | grep x:0 #查看哪些用户为root权限，有没有新增的



cat /etc/passwd | grep /bin/bash #查看哪些用户使用shell



查询可以远程登录的账号：awk ‘/\$1|\$6/{print $1}’ /etc/shadow

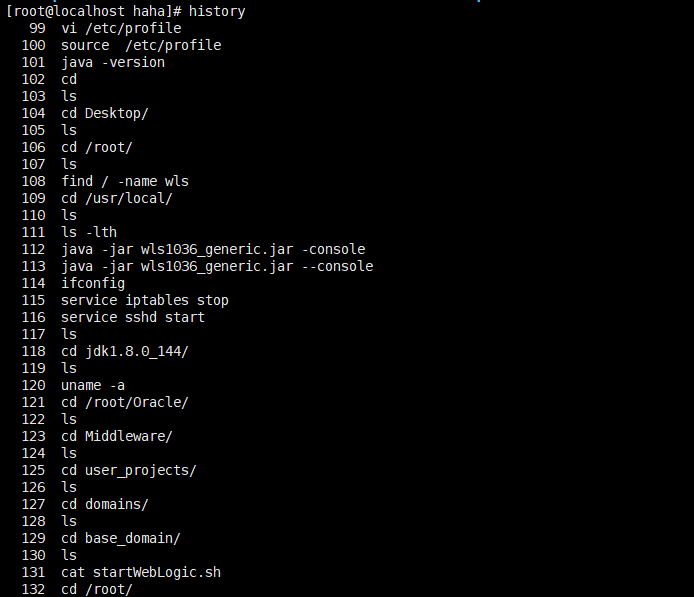
查询具有sudo权限的账号：more /etc/sudoers | grep -v “^#\|^$” grep “ALL=(ALL)”

# 2.历史命令

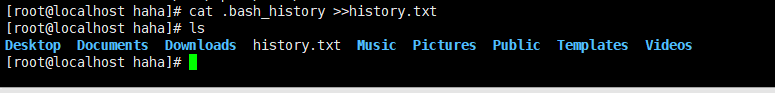
很多的服务器会有存在多用户登陆情况，登陆root用户可查看其他用户的相关账户登录信息,.bash\_history保存了用户的登陆所操作的命令信息

home/root/.bash\_history

history查看历史命令

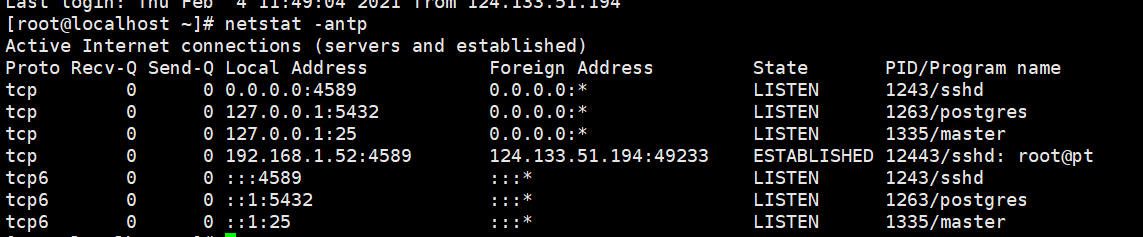


cat .bash\_history >>history.txt 保存历史命令



# 3.查看端口

netstat –antp

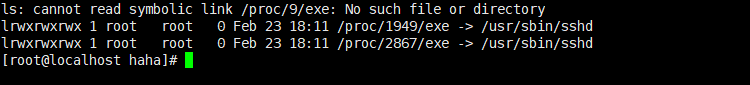


查看对应链接的文件路径

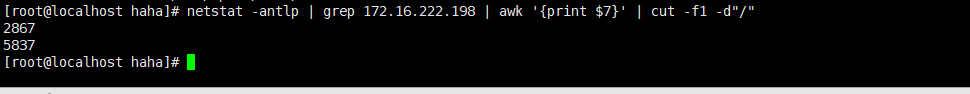
ls -l /proc/pid/exe



ls -l /proc/\*/exe | grep xxx #如果我们知道恶意程序的启动文件大致位置，可以使用这个发现无文件的恶意进程

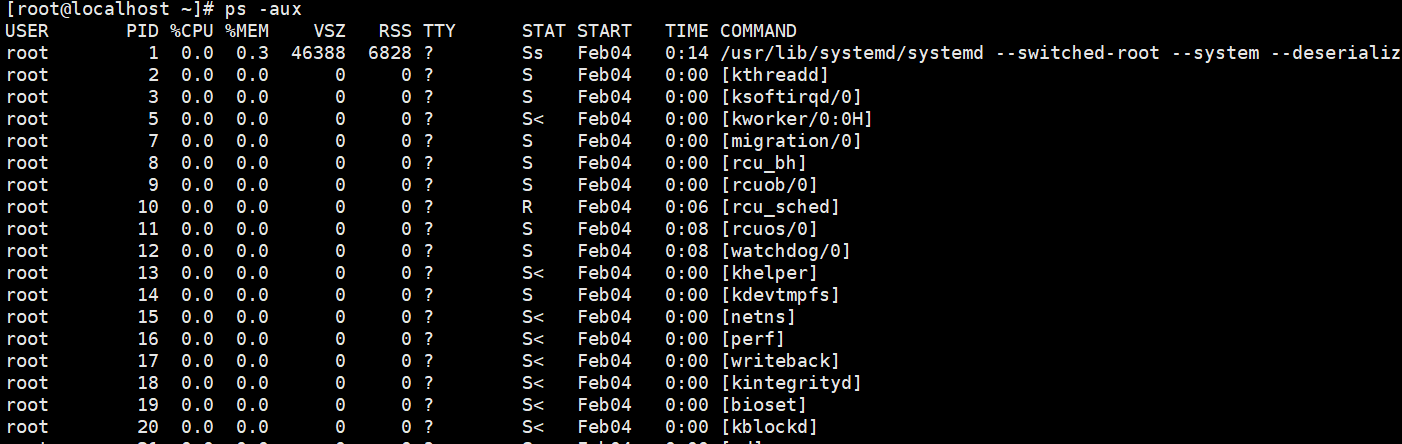


netstat -antlp | grep 172.16.222.198 | awk '{print $7}' | cut -f1 -d"/" 通过可疑的ip地址获取程序pid



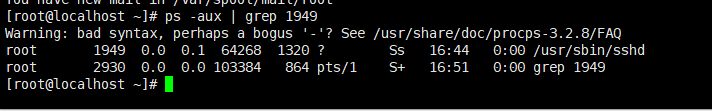
# 4.查看进程

ps -aux



查看相关pid对应程序

ps –aux | grep pid

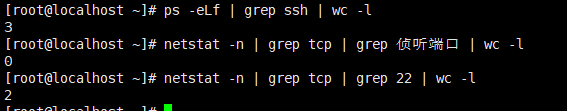


监控某一应用线程数（如ssh）

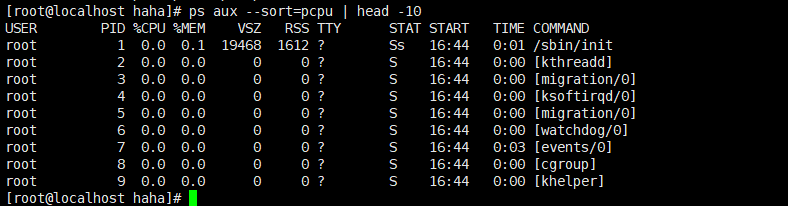
ps -eLf | grep ssh| wc –l

监控网络客户连接数

netstat -n | grep tcp | grep 侦听端口 | wc -l



ps aux --sort=pcpu | head -10 查看cpu占用率前十的进程，有时候可以发现



# 5.开机启动项

启动项文件：

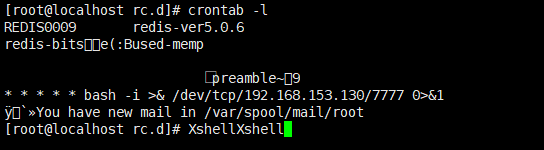
more /etc/rc.local

/etc/rc.d/rc[0~6].d

ls -l /etc/rc.d/rc3.d/

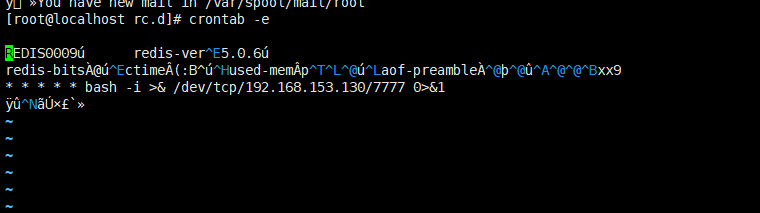
# 6.定时任务

crontab -l



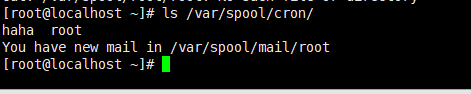
编辑定时任务

crontab –e



crontab -u root –l 查看root用户任务计划

ls /var/spool/cron/ 查看每个用户自己的执行计划



#删除计划任务且控制计划任务不能写东西

sed '/gcc.sh/d' /etc/crontab && chmod 0000 /etc/crontab && chattr +i /etc/crontab

常见的定时任务文件：

/var/spool/cron/\* #centos的

/var/spool/cron/crontabs/\* #ubuntu的

/var/spool/anacron/\*

/etc/crontab

/etc/anacrontab #异步定时

/etc/cron.hourly/\*

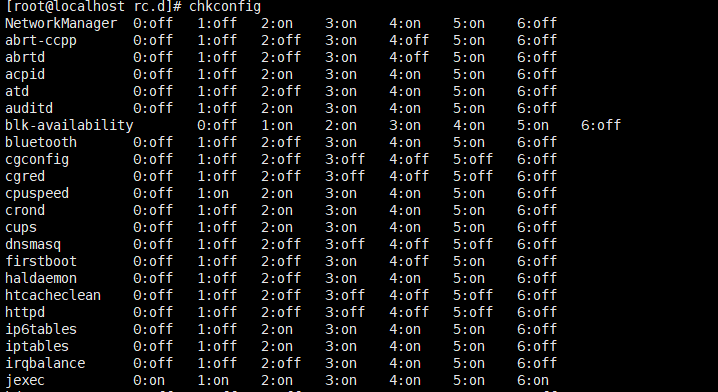
/etc/cron.daily/\*

/etc/cron.weekly/

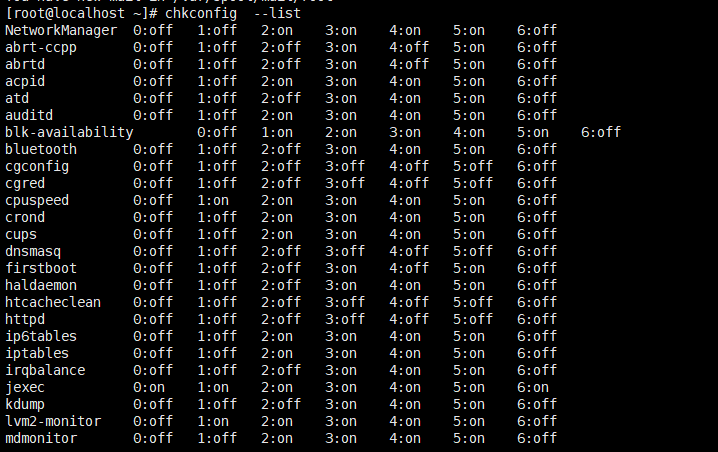
/etc/cron.monthly/\*

# 7.服务

chkconfig 查看开机启动项目



chkconfig --list 查看服务自启状态



systemctl list-unit-files |grep enabled

# 8.查找文件

find查找指定的文件：find /home1 -name \*.php ! -name index.php

find查看最近一天修改的文件: find / -mtime -1 > /etc/aa.txt(查看修改的文件并保存到aa的txt文档)

查找并删除,liyong xargs find . -name .svn | xargs rm –rf

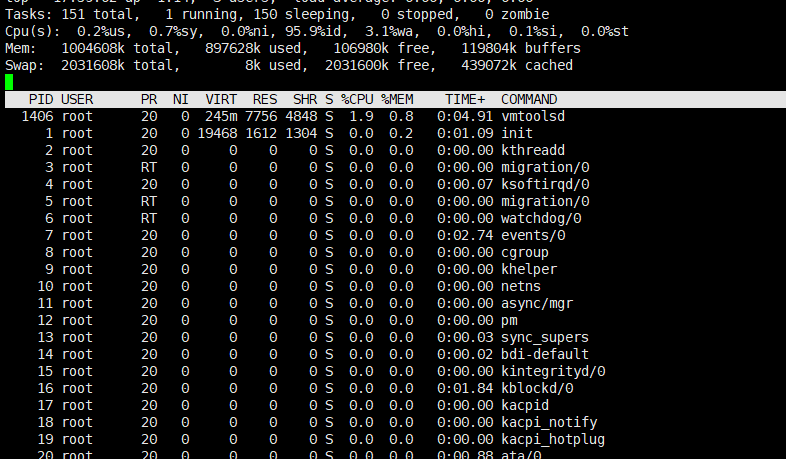
find / -size +10000k -print：查找大于10000k的文件

md5sum -b filename：查看文件的md5值

# 9.top命令

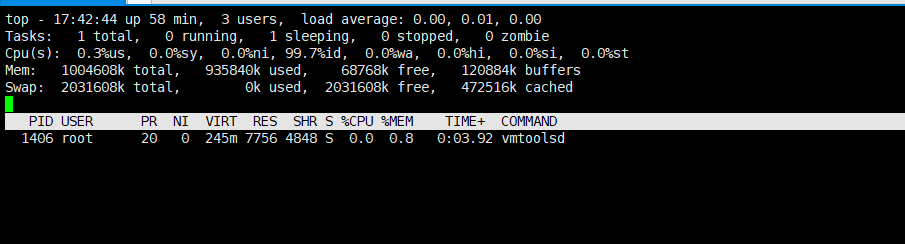
top命令是Linux下常用的性能分析工具，能够实时显示系统中各个进程的资源占用状况，类似于Windows的任务管理器。

默认top是根据cpu的占用情况进行排序的

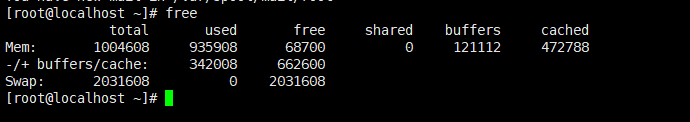


可通过按“b”键进行切换，可切换到按照内存使用情况进行排序

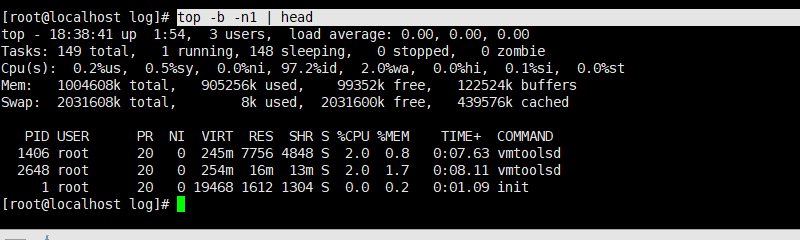
top -p pid 监控指定进程



free 查看当前系统内存使用情况

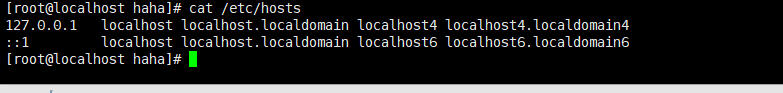


top -b -n1 | head



# 10.host文件

有一些挖矿程序会修改 /etc/hosts文件



# 11. Diff

Linux中的命令，Diff,可以查看两个文本文件的差异

# 12．日志分析

默认日志位置：var/log

1、定位有多少IP在爆破主机的root帐号：

grep "Failed password for root" /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

定位有哪些IP在爆破：

grep "Failed password" /var/log/secure|grep -E -o "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)"|uniq -c

爆破用户名字典是什么？

grep "Failed password" /var/log/secure|perl -e 'while($\_=<>){ /for(.\*?) from/; print "$1\n";}'|uniq -c|sort -nr

2、登录成功的IP有哪些：

grep "Accepted " /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

登录成功的日期、用户名、IP：

grep "Accepted " /var/log/secure | awk '{print $1,$2,$3,$9,$11}'

3、增加一个用户kali日志：

Jul 10 00:12:15 localhost useradd[2382]: new group: name=kali, GID=1001

Jul 10 00:12:15 localhost useradd[2382]: new user: name=kali, UID=1001, GID=1001, home=/home/kali

, shell=/bin/bash

Jul 10 00:12:58 localhost passwd: pam\_unix(passwd:chauthtok): password changed for kali

#grep "useradd" /var/log/secure

4、删除用户kali日志：

Jul 10 00:14:17 localhost userdel[2393]: delete user 'kali'

Jul 10 00:14:17 localhost userdel[2393]: removed group 'kali' owned by 'kali'

Jul 10 00:14:17 localhost userdel[2393]: removed shadow group 'kali' owned by 'kali'

# grep "userdel" /var/log/secure

5、su切换用户：

Jul 10 00:38:13 localhost su: pam\_unix(su-l:session): session opened for user good by root(uid=0)

sudo授权执行:

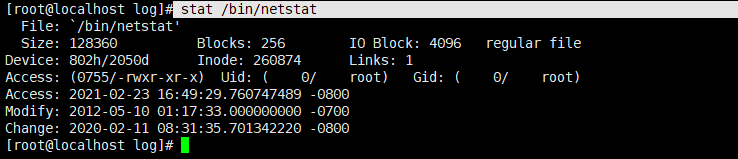
sudo -l

Jul 10 00:43:09 localhost sudo: good : TTY=pts/4 ; PWD=/home/good ; USER=root ; COMMAND=/sbin/shutdown -r now

# 13.查看命令状态

很多情况下，存在ps、netstat等一些常见命令被替换，可利用stat查看该状态，查看其修改时间

stat /bin/netstat



# 14文件清除

很多时候会遇到无法常看文件权限或是病毒在一直向某个文件写入程序，可尝试如下命令：

lsattr [恶意文件绝对路径]命令查看权限，

使用chattr -i [恶意文件绝对路径]解除文件锁定后删除。

chmod 0000 /lib/libudev.so && rm -rf /lib/libudev.so && chattr +i /lib/（chattr +i不让lib文件被写入删除）

结束某一进程：

Kill -9 pid