14.查看系统日志命令

linux系统中有很多重要的日志文件，这些文件可以保存很多访问linux的日志记录，比如登录者的信息及他们的行为，那些用户正在登陆，所有登陆过的用户信息，系统中所有用户最后一次的登陆时间，错误登陆的信息等等，我们可以通过这些日志了解用户都做了些什么，有没的黑客攻击等等。这些日志大多存放在/var/log目录下和/run目录下，但是这些日志中，有些并不是能够用cat，vi，more...这些命令能够打开的，要查看需要用到一下特殊的命令：

1.w命令

作用：

w命令->用来查看登录者的信息及他们的行为。

使用：

```
[root@localhost ~]# w
```

显示内容说明：

第一行：系统当前时间　系统的运行时间　当前登录用户数　系统在之前 1 分钟、5 分钟、15 分钟的平均负载

User：登录用户名

TTY：登录后系统分配的终端号

From：远程主机名，即从哪登录的

login@：何时登录

IDLE：用户空闲时间。这是个计时器，一旦用户执行任何操作，改计时器就会被重置。

JCPU：和终端连接的所有进程占用时间。包括当前正在运行的后台作业占用时间

PCPU：当前进程所占用时间

WHAT：当前正在运行进程的命令行

2.who 命令

作用：

who 命令显示关于当前在本地系统上的所有用户的信息。

显示以下内容：登录名、tty、登录日期和时间。

输入whoami 显示自己的登录名、tty、您登录的日期和时间。

如果用户是从一个远程机器登录的，那么该机器的主机名也会被显示出来。

使用：

```
[root@localhost ~]# who
```

3.last命令

作用：

last作用是显示近期用户或终端的登录情况。通过last命令查看该程序的log，管理员可以获知谁曾经或者企图连接系统。

使用：

指定显示记录的数量（显示记录中最后登录的数量）

last -n 10

显示内容：

第一列：用户名

第二列：终端位置（pts/0伪终端，意味着从SSH或telnet等工具远程连接的用户，图形界面终端归于此类。tty0直接连接到计算机或本地连接的用户。后面的数字代表连接编号）

第三列：登录IP或内核（如果是：0.0或者什么都没有，意味着用户通过本地终端连接。除了重启活动，内核版本会显示在状态中）

第四列：开始时间

第五列：结束时间（still login in尚未退出，down直到正常关机，crash直到强制关机）

第六列：持续时间

4. lastlog 命令

功能：

检查最后一次登录本系统的用户登录的时间信息

显示：

#用户名　　终端　　来源 IP　　登陆时间

使用：

lastlog

5.lastb 命令

功能：

lastb 命令是查看错误登陆的信息的，查看的是/var/log/btmp

使用：

lastb

显示：

#错误登陆用户　终端　　尝试登陆的时间