linux 中 shell 历史命令记录功能

投稿：hebedich 字体：[增加 减小] 类型：转载 时间：2014-10-10 我要评论

这篇文章主要介绍了在 Linux 下面可以使用 history 命令查看用户的所有历史操作的一些详细配置小技巧，非常的简单实用，有需要的朋友可以参考下

在 Linux 下面可以使用 history 命令查看用户的所有历史操作，同时 shell 命令操作记录默认保存在用户目录的 .bash_history 文件中。通过这个文件可以查询 shell 命令的执行历史，有助于运维人员进行系统审计和问题排查，同时在服务器遭受黑客攻击后，也可以查询黑客登录服务器的历史命令操作。但是黑客在入侵后，为了抹除痕迹，会删除 .bash_history 文件，这个就需要合理备份这个文件了。

默认的 history 命令只能查看用户的历史操作记录，但是不能区分每个用户操作命令的时间。这点对于问题排查相当的不方便。解决办法是在 /etc/bashrc 文件中加入以下四行来让 history 命令自动记录所有 shell 命令的执行时间：

复制代码 代码如下:

```
HISTFILESIZE=4000
HISTSIZE=4000
HISTTIMEFORMAT='%F %T'
export HISTTIMEFORMAT
```

HISTFILESIZE 表示在 .bash_history 文件中保存命令的记录总数，默认值是 1000；HISTSIZE 定义了 history 命令输出的记录总数；HISTTIMEFORMAT 定义了时间显示格式，该格式与 date 命令后的 “+"%F %T"” 是一样的；HISTTIMEFORMAT 作为 history 的时间变量将值传递给 history 命令。

高级技巧

上面那个虽然可以记录时间，但是无法作为审计目的使用，很容易被黑客篡改或者丢失。下面这种方法详细记录了登录过系统的用户、IP 地址、shell 命令以及详细操作的时间。并将这些信息以文件的形式保存在一个安全的地方，以供系统审计和故障排查。

把以下代码放入 /etc/profile 文件中，即可实现上述功能。

复制代码 代码如下:

```
#Record history operation
USER_IP=`who -u am i 2>/dev/null |awk '{print $NF}' |sed -e 's/[()]//g'`
LOGNAME=`who -u am i |awk '{print $1}'`
HISTDIR=/user/share/.history
if [ -z $USER_IP]
then
USER_IP=`hostname`
fi

if [ ! -d $HISTDIR]
then
mkdir -p $HISTDIR
chmod 777 $HISTDIR
fi

if [ ! -d $HISTDIR/${LOGNAME}]
then
```

```
mkdir -p $HISTDIR/${LOGNAME}

chmod 300 $HISTDIR/${LOGNAME}

fi


export HISTSIZE=4000


DT=`date +"%Y%m%d_%H%M%S"`

export HISTFILE="$HISTDIR/${LOGNAME}/${USER_IP}.history.$DT"

export HISTTIMEFORMAT="[%Y.%m.%d %H:%M:%S]"

chmod 600 $HISTDIR/${LOGNAME}/*.history* 2>/dev/null
```