链滴

擦屁股与审计

作者：dafsic

原文链接：https://ld246.com/article/1513672652459

来源网站：链滴

Linux上如何擦屁股与审计

概述

我们知道，当我们登陆到一台Linux机器，一顿操作后退出，我们的登陆信息被last记录、操作的命令被history记录。但有些时候（机器不是自己的），我们不想这些信息被记录。但还有些时候（机器是己的），我们希望这些信息记得更详细。

擦屁股

不要纠结为什么叫擦屁股，没上过学，词穷。总之，目的是要做到“事了拂衣去，深藏身与名”。

修改last记录

因为last记录在/var/log/wtmp 文件中，而且是非文本方式保存的，所以不能用vim直接打开编辑。

1. utmpdump /var/log/wtmp > newdump 将last日志（wtmp）转换ASCII格式并保存newdum;
2. 用vim打开newdump编辑（当然是删掉你的记录了）。
3. utmpdump -r newdump > /var/log/wtmp 将修改后的newdump文件转换成二进制并替换wtp;
4. last一下，检查

修改history记录

在这之前，也可以再改下/var/log/secure文件，正常因为这个内容很多，不方便看的，除了排错我少看它。反正，history肯定是要最后修改了，不然.....就是智障。

1. 因为是文本文件，所以直接用vim打开.bash_histo
y修改。
2. history -r .bash_history 使修改生效，-r是读的意思了。

如果，在登陆机器之前就知道要删掉记录的话，一上来就一个cp .bash_history ./aaa，把history文备份了，在退出之前mv ./aaa .bash_history，rm ./aaa，history -r .bash_history完美。

以上操作并不唯一，思路大概就这样。

审计

如果机器是自己的，我们可能就需要做审计了，总不能机器被黑了，别人在你机器上干了啥都不知道。如果都是root，到底道高一尺魔高一丈，还是魔高一尺道高一丈真不好说。但是道和魔都是少数，多数都是普通那个人，即使魔高一尺也不是普通人所能抵挡的。

虽然我说了些什么，但是不用在意我说了些什么。

记录登陆信息

1. 在/etc/rsyslog.conf文件中加入user.notice /var/log/auth.log一行；

2. touch /var/log/auth.log创建这个文件，所以文件是自定义的，与上一行的一致即可；

3. 在/etc/profile文件中加入　logger -p user.notice -- time=\"`(date -d now +"%Y-%m-%d %T")\" src_ip=\"`(who -m|cut -d\(-f2|cut -d\) -f1)`\" 2>/dev/null；

原理就是（参考下面的记录shell命令），每次登陆系统时必然会执行/etc/profile文件，文件中利用loger产生一条用户自定义的记录，这条记录要保存到哪里，这个在/etc/rsyslog.conf中指定为/var/log auth.log，即每次有用户登陆到系统，都会把时间和ip记录到/var/log/auth.log中。当然还可以记录户名、会话id等。但是/var/log/auth.log是可以被修改的，所以可以在第一步中将/var/log/auth.log为@192.168.1.2，即将这条记录发送到其他机器上（查rsyslog用法），实时的无法改的。

记录shell命令

1. 在/etc/rsyslog.conf文件中加入local1.notice /var/log/history.log一行；

2. touch /var/log/hsitory.log创建这个文件。

3. 在/etc/profile文件中加入　export PROMPT_COMMAND='{ cmd=$(history 1 | { read a b; ech "$b"; });msg=$(who am i |awk "{print \$2,\$5}");logger -i -p local1.notice "$msg $USER $PWD # $cmd"; }'

原理跟上面的类似，这里因为要记录所有用户的所有操作，所以不是登陆时产生一条记录就可以的。里用到了PROMPT_COMMAND这个shell内置的变量，会在PS1之前执行这个变
所代表的命令。这个命令就是用logger产生一条记录。

总结

记录shell中有个问题，如果别人把命令写到脚本里甚至写到程序里，记录的只是看到执行了一个脚本名字，里面是什么就不知道了。比如，之前的redis漏洞，能通过redis写一个ssh key到你的机器上，后直接登陆到主机。这个写key的过程是审计不到的，所以这时需要更高级的审计方法。

要审计系统调用，可以用一个内核模块audit。看起来能满足要求，不过这个我也没用过，没有调查没有发言权。另外，谁有什么相关的奇技淫巧也可以告诉我。