链滴

4- 文件完整性检查和 sudo

作者：Carey

原文链接：https://ld246.com/article/1610714519350

来源网站：链滴

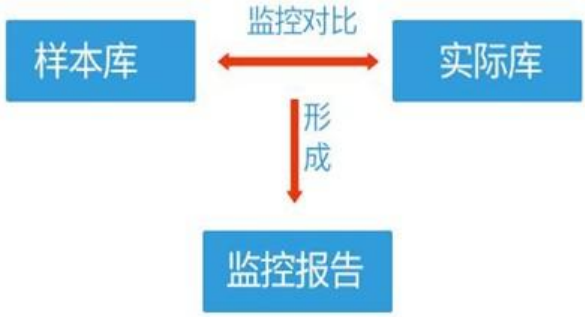
许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

4 文件完整性检查AIDE(Advanced Intrusion Detection Environment)

当一个入侵者进入了你的系统并且种植了木马，通常会想办法来隐蔽这个木马（除了木马自身的一些隐蔽特性外，他会尽量给你检查系统的过程设置障碍），通常入侵者会修改一些文件，比如管理员通常ps aux来查看系统进程，那么入侵者很可能用自己经过修改的ps程序来替换掉你系统上的ps程序，使用ps命令查不到正在运行的木马程序。如果入侵者发现管理员正在运行crontab作业，也有可能替掉crontab程序等等。所以由此可以看出对于系统文件或是关键文件的检查是很必要的。目前就系统完整性检查的工具用的比较多的有两款：Tripwire和AIDE，前者是一款商业软件，后者是一款免费的但能也很强大的工具

AIDE(Advanced Intrusion Detection Environment高级入侵检测环境)是一个入侵检测工具，主要途是检查文件的完整性，审计计算机上的那些文件被更改过了

AIDE能够构造一个指定文件的数据库，它使用aide.conf作为其配置文件。AIDE数据库能够保存文件的各种属性，包括：权限(permission)、索引节点序号(inode number)、所属用户(user)、所属用户组group)、文件大小、最后修改时间(mtime)、创建时间(ctime)、最后访问时间(atime)、增加的大小以及连接数。AIDE还能够使用下列算法：sha1、md5、rmd160、tiger，以密文形式建立每个文件的验码或散列号



这个数据库不应该保存那些经常变动的文件信息，例如：日志文件、邮件、/proc文件系统、用户起始

目录以及临时目录

安装AIDE

[17:43:01 root@centos8 ~]#yum install aide

配置文件指定对那些文件进行检测

[17:43:34 root@centos8 ~]#vim /etc/aide.conf

配置范例：

```
#定义监控项权限+索引节点+链接数+用户+组+大小+最后一次修改时间+创建时间+md5校验值
R=p+i+n+u+g+s+m+c+md5
NORMAL = R+rmd60+sha256
/data/test.txt R
/bin/ps R+a
/usr/bin/crontab R+a
/etc    PERMS
!/etc/mtab   # “!”表示忽略这个文件的检查
```

初始化默认的AIDE的库：

[17:46:30 root@centos8 ~]#aide -i | --init

生成检查数据库（建议初始数据库存放到安全的地方）

[17:54:00 root@centos8 ~]#cd /var/lib/aide/
[17:55:03 root@centos8 aide]#mv aide.db.new.gz aide.db.gz

检测

[17:55:26 root@centos8 aide]#aide -C | --check

更新数据库

[17:58:44 root@centos8 ~]#aide -u | --update

5 利用 sudo 实现授权

5.1 sudo介绍

sudo 即superuser do，允许系统管理员让普通用户执行一些或者全部的root命令的一个工具，如hal ，reboot，su等等。这样不仅减少了root用户的登录 和管理时间，同样也提高了安全性

在最早之前，一般用户管理系统的方式是利用su切换为超级用户。但是使用su的缺点之一在于必须要告知超级用户的密码。sudo于1980年前后推出，sudo使一般用户不需要知道超级用户的密码即可获权限。首先超级用户将普通用户的名字、可以执行的特定命令、按照哪种用户或用户组的身份执行等信 息，登记在特殊的文件中（通常是/etc/sudoers），即完成对该用户的授权（此时该用户称为“sudo r”）；在一般用户需要取得特殊权限时，其可在命令前加上“sudo”，此时sudo将会询问该用户自的密码（以确认终端机前的是该用户本人），回答后系统即会将该命令的进程以超级用户的权限运 行之后的一段时间内（默认为5分钟，可在/etc/sudoers自定义），使用sudo不需要再次输入密码。

由于不需要超级用户的密码，部分Unix系统甚至利用sudo使一般用户取代超级用户作为管理帐号，

如Ubuntu、Mac OS X等。

sudo特性：

● sudo能够授权指定用户在指定主机上运行某些命令。如果未授权用户尝试使用 sudo，会提示联系理员

● sudo提供了丰富的日志，详细地记录了每个用户干了什么。它能够将日志传到中心主机或者日志服器

● sudo使用时间戳文件来执行类似的“检票”系统。当用户调用sudo并且输入它的密码时，用户获了一张存活期为5分钟的票

● sudo的配置文件是sudoers文件，它允许系统管理员集中的管理用户的使用权限和使用的主机。它存放的位置默认是在/etc/sudoers，属性必须为0440

5.2 sudo组成

包：sudo

配置文件：/etc/sudo.conf

授权规则配置文件：

/etc/sudoers
/etc/sudoers.d

安全编辑授权规则文件和语法检查工具

/usr/sbin/visudo

范例：

#检查语法
[18:41:09 root@centos8 etc]#visudo -c
#检查指定配置文件语法
[18:43:07 root@centos8 etc]#visudo -f /etc/sudoers.d/test

5.3 sudo命令

sudo命令
ls -l /usr/bin/sudo
sudo -i -u wang 切换身份功能和 su 相似,但不一样,sudo必须提前授权,而且要输入自已的密码
sudo [-u user] COMMAND

-V 显示版本信息等配置信息
-u user 默认为root
-l,ll 列出用户在主机上可用的和被禁止的命令
-v 再延长密码有效期限5分钟,更新时间戳
-k 清除时间戳（1970-01-01），下次需要重新输密码
-K 与-k类似，还要删除时间戳文件
-b 在后台执行指令
-p 改变询问密码的提示符号
示例：-p "password on %h for user %p: "

5.4 sudo授权规则配置

配置文件格式说明：/etc/sudoers, /etc/sudoers.d/

配置文件中支持使用通配符 glob

? 任意单一字符

* 匹配任意长度字符
[wxc] 匹配其中一个字符
[!wxc] 除了这三个字符的其它字符
\x 转义
[[alpha]] 字母

范例：

/bin/ls [[alpha]]*

配置文件规则有两类

- 别名定义：部署必须的
- 授权规则：必须的

sudoers授权规则格式：

用户 登入主机=(代表用户) 命令
user host=(runas) command

范例：

root ALL=(ALL) ALL

格式说明：

user: 运行命令者的身份
host: 通过哪些主机
(runas)：以哪个用户的身份
command: 运行哪些命令

sudoers的别名

User和runas:
username
  #uid
  %group_name
  %#gid
  user_alias|runas_alias
host:
  ip 或 hostname
  network(/netmask)
  host_alias
command:
  command name
  directory s

udoedit
Cmnd_Alias

sudo别名有四种类型：

- User_Alias
- Runas_Alias
- Host_Alias
- Cmnd_Alias

别名格式：

[A-Z]([A-Z][0-9]_)*

别名定义：

Alias_Type NAME1 = item1,item2,item3 : NAME2 = item4, item5

5.5 实战案例

案例1：

```
zhang ALL=(ALL) ALL
%cy ALL=(ALL) ALL
```

案例2：

```
zhang ALL=(root) /sbin/pidof,/sbin/ifconfig      #zhang只能执行后面俩个命令时使用root身份
%cy ALL=(ALL) NOPASSWD:ALL                       #cy组执行sudo时不需要输入密码
```

案例3：

```
User_Alias NETADMIN= zhang,cy                        #定义别名用户
Cmnd_Alias NETCMD=/usr/sbin/ip,/usr/sbin/ifconfig      #定义别名命令
NETADMIN ALL=(root) NETCMD                            #使用
```

案例4：

```
User_Alias NETADMIN= zhang,%cy
User_Alias DISKADER= tom
Host_Alias SERS=192.168.10.0/24
Runas_Alias OP=root
Cmnd_Alias NETCMD=/usr/sbin/ip,/usr/bin/cat
Cmnd_Alias DSKCMD=/usr/bin/passwd
NETADMIN SERS= NETCMD
DISKADER ALL=(OP) DSKCMD
```

案例5：

```
User_Alias ADMINUSER = adminuser1,adminuser2
Cmnd_Alias ADMINCMD = /usr/sbin/useradd，/usr/sbin/usermod, /usr/bin/passwd [a- zA-Z]*
 !/usr/bin/passwd root
ADMINUSER ALL=(root) NOPASSWD:ADMINCMD，PASSWD:/usr/sbin/userdel
```

案例6：

```
Defaults:wang runas_default=tom          #wang执行sudo默认用户是tom
wang ALL=(tom,jerry) ALL

wang$ sudo   cmd  #默认代表tom执行cmd
wang$ sudo -u jerry cmd
```

案例7：修改验证密码间隔为2分

```
[11:57:37 root@centos8 ~]#vim /etc/sudoers
Defaults    env_reset,timestamp_timeout=2

[14:25:17 root@centos8 ~]#sudo -V
```

案例8：修改ubuntu的visudo的默认编辑器

```
export EDITOR=vim
visudo
```

案例9：删除时间戳文件

```
[14:28:13 root@centos8 ~]#su - cy
Last login: Thu Jan 14 14:24:03 CST 2021 on pts/0
[cy@centos8 ~]$ sudo -K
[cy@centos8 ~]$ exit
logout
[14:28:33 root@centos8 ~]#ll /run/sudo/ts/
total 0
[14:28:45 root@centos8 ~]#ll /run/sudo/ts
total 0
```

案例10：bug思考

```
[20:12:17 root@centos8 ~]#cat /etc/sudoers.d/zhang
zhang ALL=(ALL) NOPASSWD:/usr/bin/cat  /var/log/messages*

#没有设置其他文件但是借助设置的文件可以查看其他文件
[20:12:48 root@centos8 ~]#su - zhang
[zhang@centos8 ~]$ sudo cat /etc/shadow
[sudo] password for zhang:
Sorry, user zhang is not allowed to execute '/bin/cat /etc/shadow' as root on centos8.
[zhang@centos8 ~]$ sudo cat /var/log/messages /etc/shadow | tail -1
testuser:$6$mNCi0TvEDAYPgJma$cCyVgtj8Q3ItIDNoxDUKCX2ecWHiJ/WISzlM6ybIwFCypWJt1
L5YeSm.z5PWMmaTRzSJhKgGvAMitFogwmho1:18641:0:99999:7:::

#解决方法：！表示不是排除
zhang ALL=(ALL) NOPASSWD: /usr/bin/cat  /var/log/messages*,!/usr/bin/cat  /var/log/messa
es* *
```