## **使用AIDE做入侵检测**

### **2.1 问题**

本案例要求熟悉Linux主机环境下的常用安全工具，完成以下任务操作：

1. 安装aide软件
2. 执行初始化校验操作，生成校验数据库文件
3. 备份数据库文件到安全的地方
4. 使用数据库执行入侵检测操作

### **2.2 方案**

Aide通过检查数据文件的权限、时间、大小、哈希值等，校验数据的完整性。

使用Aide需要在数据没有被破坏前，对数据完成初始化校验，生成校验数据库文件，在被攻击后，可以使用数据库文件，快速定位被人篡改的文件。

### **2.3 步骤**

实现此案例需要按照如下步骤进行。

步骤一：部署AIDE入侵检测系统

1）安装软件包

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# yum -y install aide

[root@proxy ~]# yum -y install aide

2) 修改配置文件

确定对哪些数据进行校验，如何校验数据

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# vim /etc/aide.conf
2. @@define DBDIR /var/lib/aide                            //数据库目录
3. @@define LOGDIR /var/log/aide                            //日志目录
4. database\_out=file:@@{DBDIR}/aide.db.new.gz                //数据库文件名
5. //一下内容为可以检查的项目（权限，用户，组，大小，哈希值等）
6. #p: permissions
7. #i: inode:
8. #n: number of links
9. #u: user
10. #g: group
11. #s: size
12. #md5: md5 checksum
13. #sha1: sha1 checksum
14. #sha256: sha256 checksum
15. DATAONLY = p+n+u+g+s+acl+selinux+xattrs+sha256
16. //以下内容设置需要对哪些数据进行入侵校验检查
17. //注意：为了校验的效率，这里将所有默认的校验目录与文件都注释
18. //仅保留/root目录，其他目录都注释掉
19. /root DATAONLY
20. #/boot NORMAL                                    //对哪些目录进行什么校验
21. #/bin NORMAL
22. #/sbin NORMAL
23. #/lib NORMAL
24. #/lib64 NORMAL
25. #/opt NORMAL
26. #/usr NORMAL
27. #!/usr/src                                        //使用[!]，设置不校验的目录
28. #!/usr/tmp

[root@proxy ~]# vim /etc/aide.conf

@@define DBDIR /var/lib/aide //数据库目录

@@define LOGDIR /var/log/aide //日志目录

database\_out=file:@@{DBDIR}/aide.db.new.gz //数据库文件名

//一下内容为可以检查的项目（权限，用户，组，大小，哈希值等）

#p: permissions

#i: inode:

#n: number of links

#u: user

#g: group

#s: size

#md5: md5 checksum

#sha1: sha1 checksum

#sha256: sha256 checksum

DATAONLY = p+n+u+g+s+acl+selinux+xattrs+sha256

//以下内容设置需要对哪些数据进行入侵校验检查

//注意：为了校验的效率，这里将所有默认的校验目录与文件都注释

//仅保留/root目录，其他目录都注释掉

/root DATAONLY

#/boot NORMAL //对哪些目录进行什么校验

#/bin NORMAL

#/sbin NORMAL

#/lib NORMAL

#/lib64 NORMAL

#/opt NORMAL

#/usr NORMAL

#!/usr/src //使用[!]，设置不校验的目录

#!/usr/tmp

步骤二：初始化数据库，入侵后检测

1）入侵前对数据进行校验，生成初始化数据库

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# aide --init
2. AIDE, version 0.15.1
3. AIDE database at /var/lib/aide/aide.db.new.gz initialized.
4. //生成校验数据库，数据保存在/var/lib/aide/aide.db.new.gz

[root@proxy ~]# aide --init

AIDE, version 0.15.1

AIDE database at /var/lib/aide/aide.db.new.gz initialized.

//生成校验数据库，数据保存在/var/lib/aide/aide.db.new.gz

2）备份数据库，将数据库文件拷贝到U盘（非必须的操作）

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# cp /var/lib/aide/aide.db.new.gz /media/

[root@proxy ~]# cp /var/lib/aide/aide.db.new.gz /media/

3）入侵后检测

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# cd /var/lib/aide/
2. [root@proxy ~]# mv aide.db.new.gz aide.db.gz
3. [root@proxy ~]# aide --check                            //检查哪些数据发生了变化