ADVANCE INTRUSION DETECTION ENVIRONMENT IN CENTOS SERVER

Any person who have knowledge about IT knows that “No system is 100% secure”.In today’s IT world maintaining server security is one of the biggest challenge , even the best available security is insufficient for the latest vulnerabilities in various products, and against malware/attacks created to target those vulnerabilities. While cyber-security cannot be 100 per cent fool-proof, we can still try to achieve the maximum security possible.unauthorised intrusion in the system is one of the biggest problem ,detecting attackers and the unauthorised access to a server is one of the most important work for a server admin. Because having basic security only gives you the misleading feeling of being secure, rather than actual security. Modern attackers are experts who exploit software vulnerabilities by using technical tools, and devise methods to break into a network to achieve their goals. To handle smart attack attempts, an even smarter security mechanism is needed, Thats why checking system integrity and and detecting intrusion is very important.For checking integrity in linux server we use a packages called AIDE(Advance Intrusion Detection Environment).Its a file and directory integrity checker.

What does it do?

It creates a database from the regular expression rules that finds from the config files.Once the database is created it is used to check the the intrigrity of the files.It uses several message digest algorithm that are used to check the integrity of the file.and they can detect the version of files

Features

- supported message digest algorithms: md5, sha1, rmd160, tiger, crc32, sha256, sha512, whirlpool (additionally with libmhash: gost, haval, crc32b)

- supported file attributes: File type, Permissions, Inode, Uid, Gid, Link name, Size, Block count, Number of links, Mtime, Ctime and Atime
- support for Posix ACL, SELinux, XAttrs and Extended file system attributes if support is compiled in
- plain text configuration files and database for simplicity
- powerful regular expression support to selectively include or exclude files and directories to be monitored
- gzip database compression if zlib support is compiled in
- stand alone static binary for easy client/server monitoring configurations

SETTING UP AIDS IN CENTOS SERVER

1)give the server a static ip address.

centos server ip address:

ip:192.168.0.100
subnet mask:255.255.255.0
gateway:192.168.0.1
dns:8.8.8.8

your ip address cen be different.

2) update the repository of the centos

=>**yum update**

3) install the epel-release

=>yum install epel-release -y
=>yum update

4)install the aide package

```
=> yum install aide -y
```

5) Create the database

```
=>aide –init
```

[This may take some time]

6) Once the database is created you can move and rename it like the original one to make it work

```
=>mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

TESTING THE APPLICATION

7) For Testing we make a binary file inside the **'/usr/sbin'** directory

```
=>touch /usr/bin/testbin
```

8) Check the database again

```
=>aide –check
```

lets see the output;

```
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2019-08-26 07:19:13

Summary:
  Total number of files:160184
  Added files:          2
  Removed files:        0
  Changed files:    0
---------------------------------------------------
Added files:
---------------------------------------------------
```

```
added: /sbin/testbin
added: /usr/sbin/testbin
```

[add pic for that]

9)So we can see aide can detect the change of the file.

10) if you think this file is not dangerous you can add the file the database so in the next search it will not be shown. Update the database with this command

=>aide –update

[pic]

SETTING UP AIDE IN DEBIAN SERVER

---

1)give the server a static ip address.

centos server ip address:

ip:192.168.0.100
subnet mask:255.255.255.0
gateway:192.168.0.1
dns:8.8.8.8

your ip address can be different.

2) update the repository of the debian

=>**apt update**

3) install the aide package
=> apt install aide -y

[remember aide need additional packages to work.So make sure you install the packages through apt]

5) Create the database

```
=>aideinit
```

[This may take some time]

6) Once the database is created you can copy and rename it like the original one to make it work

```
=>cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db
```

7) now we need to update the configuration file

```
=>update-aide.conf
```

8) The newly genaerated configuration file is stored in '**/var/lib/aide/aide.conf.autogenerated**' name.

9) we need to copy the configuration file to the '**/etc/aide/aide.conf'** name to **'/etc/aide'** directory

```
=>cp /var/lib/aide/aide.conf.autogenerated /etc/aide/aide.conf
```

10) check the database
syntax: **aide -c <conf file> --check**

```
=> aide -c /etc/aide/aide.conf --check
```

11) For Testing we make a binary file inside the **'/usr/sbin'** directory

```
=>touch /usr/bin/testbin
```

8) Check the database again

=>aide -c /etc/aide/aide.conf –check

9)So we can see aide can detect the change of the file.

10) if you think this file is not dangerous you can add the file the database so in the next search it will not be shown. Update the database with this command

=>aids –update

[pic]