Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Debian / Ubuntu Linux Install Advanced Intrusion Detection Environment (AIDE) Software

Posted by Vivek Gite <vivek@nixcraft.com>


[1]

AIDE is an open source host-based intrusion detection system which is a replacement for the well-known Tripwire integrity checker. It provide software integrity checking and it can detect that intrusions (monitor filesystem for unauthorized change such as find out if system binaries modified and a new cracked versions installed or not) have occurred on the system. How do I install and configure AIDE under Ubuntu LTS / Debian Linux 5.0 server?

It is a good practice to deploy any integrity checking software before system goes online in a production environment. If possible install this software before the system is connected to any network. AIDE is a host-based intrusion detection system (HIDS) it can monitor and analyses the internals of a computing system.

1.0 Debian / Ubuntu Linux Install AIDE

Type the following command:

```
# apt-get update && apt-get install aide
```

1.0.1 Configure and Customize AIDE

You need to customize /etc/aide/aide.conf to meet your requirements. The default configuration is acceptable for many environments.

- /etc/aide/aide.conf and /etc/aide/aide.conf.d/ - Default AIDE configuration files.
- /var/lib/aide/aide.db - Default location for AIDE database.
- /var/lib/aide/aide.db.new - Default location for newly-created AIDE database.

1.0.2 How Do I Build, Store, and Test Database?

aideinit creates a new AIDE database. It will initialize an AIDE database in the default database_out location (defined in /etc/aide/aide.conf). It will then prompt you to replace your existing AIDE database. aideinit attempts to automatically detect the correct locations of your database and database_out files based on your aide.conf settings. These settings may be overriden on the command line, as may the prompts. To generate a new database, enter:

```
# aideinit
```

Sample output:

```
Running aide --init...
```

Sample output:

```
AIDE, version 0.13.1
### AIDE database at /var/lib/aide/aide.db.new initialized.
```

Finally, install the newly-generated database, enter:

```
# cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db
```

Next, run a manual check:

```
# aide -c /etc/aide/aide.conf --check
```

If this check produces any unexpected output, investigate. You need to move the database, as well as the configuration

file /etc/aide/aide.conf and the aide binary to a secure offsite readonly location. This should be done to improve overall security. If attacker can modify the binary then you would not spot anything, so move it out or burn the files to the CD-ROM and use that for the checking. You can also use hashes of these files. Move files to offsite server.

```
# scp /var/lib/aide/aide.db* /usr/bin/aide /etc/aide/aide.conf /etc/aide/aide.conf.d/*
user@offsite.server.com:/path/to/dir
```

Use tools such as cdrecord to write the [2] files on CDROM.

1.0.4 How Do Test Integrity of Any Binary?

Run the command (note: usually you only need to run aide -c /etc/aide/aide.conf --check):

```
# touch /bin/date
# aide -c /etc/aide/aide.conf --check
```

1.0.5 Cron To Implement Periodic Execution of Integrity Checking

By default, AIDE install itself for periodic execution at /etc/cron.daily/aide. This script will get executed once a day, which may be suitable for many server environments. If there is any problem with installed binaries (modified by you or a system update program such as apt-get or by an attacker), you will get an email (default sent to root user). You can customize email by editing /etc/default/aide file. You need to set MAILTO variable. This is the email address reports get mailed.

```
MAILTO=vivek@nixcraft.co.in
```

1.0.6 A Note About System Changes

AIDE mail may be an indication of an attack against your server. However, sometime you update system and configuration change or a software update. The following steps
should be repeated when configuration changes or software updates necessitate:

```
# aideinit
# cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db
# aide -c /etc/aide/aide.conf --check
```

Finally, move the files (database and aide binary) to readonly media or offsite server using scp (see steps described in section #1.02 [3]) .

Further Readings:

- The man page aide.conf(5) provides detailed information about the configuration file format.
- The man page aide(1) provides detailed information about the aide command options.
- AIDE project home page [4]