

System Integrity and Intrusion Detection

- Install And Configure Fail2Ban
- Install And Configure AIDE

Install And Configure Fail2Ban

Add sudo in front of the commands if you are using a normal account with sudo privileges

Installation

1. Run the command below to install Fail2Ban

```
apt-get install fail2ban -y
```

Configuration

1. Copy the "jail.conf" file and re-save it with the name "jail.local"

```
cp -pf /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

2. Edit the jail.local and add your local IP address onto the **ignoreip** line

```
[ DEFAULT ]
```

```
# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will not
# ban a host which matches an address in this list. Several addresses can be
# defined using space separator.
```

```
ignoreip = 127.0.0.1
```

```
# Override /etc/fail2ban/jail.d/00-firewalld.conf:
```

```
banaction = iptables-multiport
```

```
# "bantime" is the number of seconds that a host is banned.
```

```
bantime = 600
```

```
# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
```

```
findtime = 600
```

```
# "maxretry" is the number of failures before a host get banned.  
maxretry = 5
```

Add a jail file to protect SSH access

1. Create a new file called sshd.local

```
| touch /etc/fail2ban/jail.d/sshd.local && chmod +x /etc/fail2ban/jail.d/sshd.local |
```

2. Edit the file and add the lines below

```
vi /etc/fail2ban/jail.d/sshd.local
```

Add these lines to the file

```
=====
```

```
[sshd]  
enabled = true  
port = ssh  
#action = firewallcmd-ipset  
logpath = %(sshd_log)s  
maxretry = 5  
bantime = 86400
```

Enable and start the FAIL2BAN service

1. Run the following commands to enable and start the Fail2Ban service

```
systemctl enable fail2ban  
systemctl start fail2ban
```

Install And Configure AIDE

Add sudo in front of the commands if you are using a normal account with sudo privileges

Install and configure Host Based IDS (Intrusion Detection System) "AIDE"

1. Install AIDE

```
apt-get install aide -y
```

2. Configure AIDE and initialize database. It's possible to use AIDE with default config but if you'd like to customize settings, change configuration file like follows. Setting rules are written near 26-84 lines, refer to them.

```
[root@dlp ~]# vi /etc/aide.conf

# for example, change setting of monitoring /var/log
/var/log p+u+g+i+n+a+c+l+selinux+xattrs

# initialize database
[root@dlp ~]# aide --init

AIDE, version 0.15.1

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

# copy generated DB to master DB
[root@dlp ~]# cp -p /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

3. Execute checking

```
[root@dlp ~]# aide --check
# if there is no unmatched, it displays "Okay"

AIDE, version 0.15.1

### All files match AIDE database. Looks okay!

# try to change a file and check again
[root@dlp ~]# chmod 640 /root/anaconda-ks.cfg
[root@dlp ~]# aide --check
```

```
# detected differences like follows
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2015-06-17 19:55:20
```

Summary:

Total number of files:	39039
Added files:	0
Removed files:	0
Changed files:	1

Changed files:

changed: /root/anaconda-ks.cfg

Detailed information about changes:

File: /root/anaconda-ks.cfg

Perm	: -rw-----	, -rw-r-----
Ctime	: 2015-05-24 02:22:04	, 2015-06-19 11:55:15
ACL	: old = A:	

user::rw-
group:---
other:---

D: <NONE>
new = A:

user::rw-
group:r--
other:---

D: <NONE>

Update AIDE database

1. If there is no problem even if some differences are detected, then update database like follows

```
[root@dlp ~]# aide --update
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2015-06-17 19:56:31

Summary:
  Total number of files:      39039
  Added files:                0
  Removed files:              0
  Changed files:              1

-----
Changed files:
-----

changed: /root/anaconda-ks.cfg
.....
.....

# update database
[root@dlp ~]# cp -p /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

Add Cron job and email logs

1. Add in Cron if check regularly. Log file [/var/log/aide/aide.log] is updated every time and if there is no difference, it is updated with zero byte, so if you's like to save log files, it needs to create a shell script or send results via email or others

```
# for example, add daily check in Crontab and send results via email

[root@dlp ~]# vi /etc/cron.d/aide
00 01 * * * /usr/sbin/aide --update | mail -s 'Daily Check by AIDE' root
```