AlienVault: End user Devices Integration-Lab Setup (Part 2)

October 13, 2020 By Raj Chandel

As logs never lie, it's very important to aggregate and analyze the internal and external network logs constantly so that you can prevent a breach or perform incident response on time. In the **previous article**, we looked at the configuration and installation of AlienVault OSSIM.

The operating-system integration for AlienVault is based on window-centric for a Linux platform.

Let's take a look at the involved process for gathering logs from Linux servers using AlienVault.

You can access the previous article from here: – **AlienVault Lab setup**

in this article, we will discuss how to send Ubuntu RSYS logs to the AlienVault server and the Manual configuration and installation of the SSH plugin.

So, without much theory let's begin the integration process.

Table of Content

Prerequisites

For the integration of Rsyslog and SSH plugin to AlienVault OSSIM, there are some minimum requirements as listed below.

- Ubuntu 20.04 or later
- Root privileges

Credentials

- Ubuntu 20.04 IP: 192.168.1.8
- AlienVault OSSIM IP: 192.168.1.70
- OSSIM (CLI) user: root
- OSSIM password: Designated by you on the time of server setup

Integration of Rsyslog and SSH plugin to AlienVault OSSIM

Ubuntu 20.04

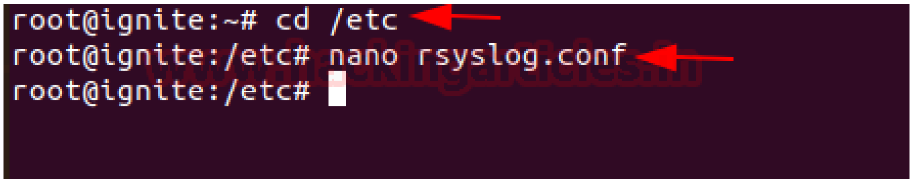
Rsyslog is a software that is used for forwarding log messages in an IP network. It implements basic Syslog protocol and extends it with content-based filtering capabilities. It also supports different module outputs, flexible configuration options and adds features such as TCP for transport.

Make sure the Port 514 (UDP protocol) is both on the ubuntu 20.04 server-side and AlienVault OSSIM server is open so that the logs can be forwarded via UDP on port 514

Open rsyslog.conf file and check whether it is including all configuration file or not

To do this enter the following command

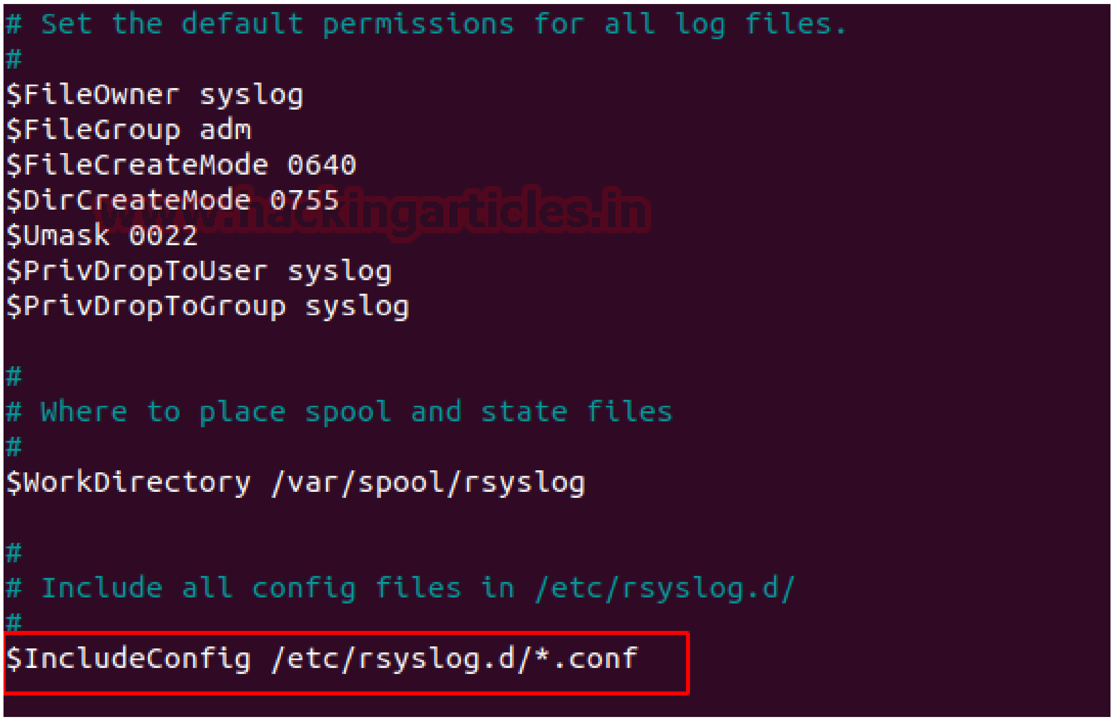
```
cd /etc
nano rsyslog.conf
```



```
root@ignite:~# cd /etc
root@ignite:/etc# nano rsyslog.conf
root@ignite:/etc#
```

Uncomment the following line to include all configuration files.

```
$IncludeConfig /etc/rsyslog.d/*.conf
```



```
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
```

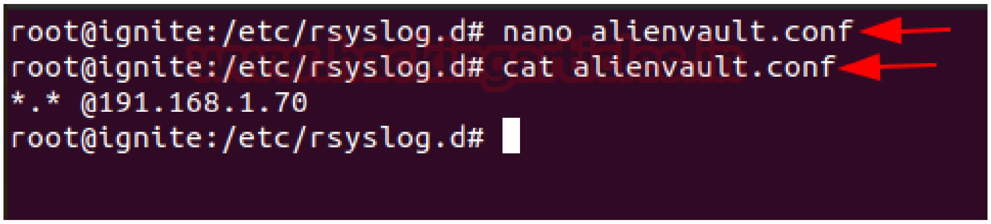
If this line by default is uncommented, then save and exit.

Now we forward the rsyslog logs to the AlienVault OSSIM server.

Create a new configuration file named alienvault.conf and add the following line as shown below:

```
nano alienvault.conf
*.* @192.168.1.70
```

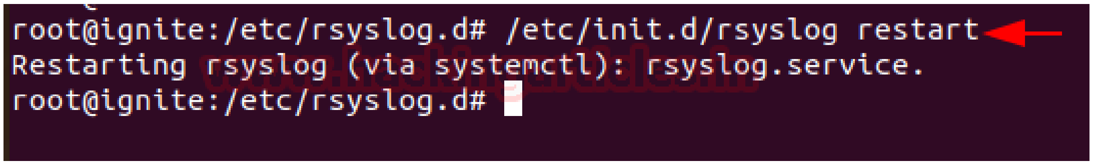
Where 192.168.1.70 is OSSIM server IP.



```
root@ignite:/etc/rsyslog.d# nano alienvault.conf
root@ignite:/etc/rsyslog.d# cat alienvault.conf
*.* @191.168.1.70
root@ignite:/etc/rsyslog.d#
```

To make the changes effective restart rsyslog service by the following command:

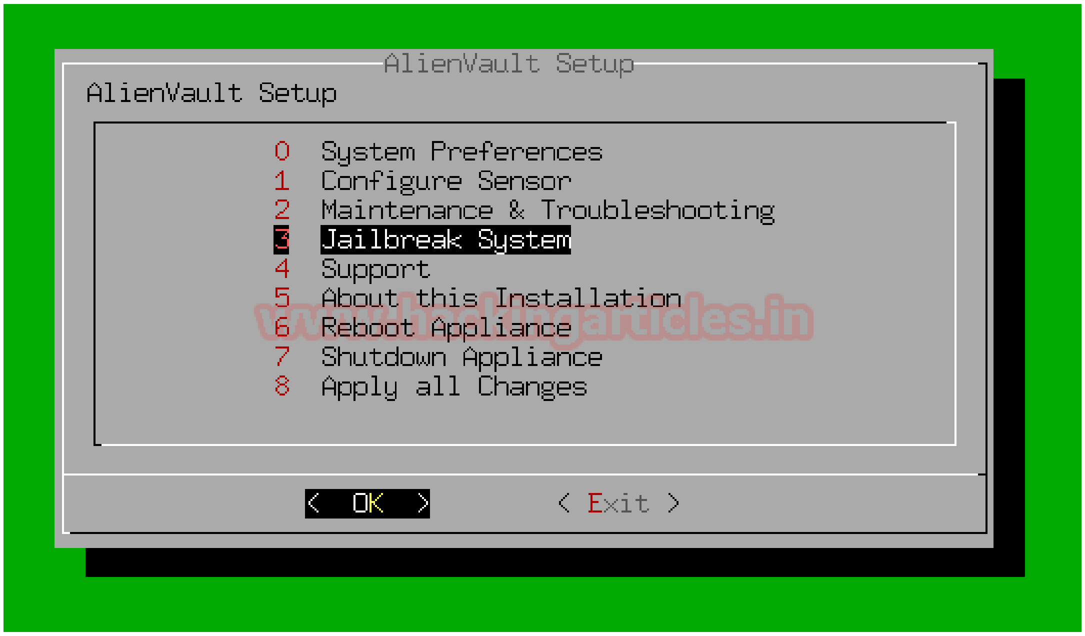
```
/etc/init.d/rsyslog restart
```



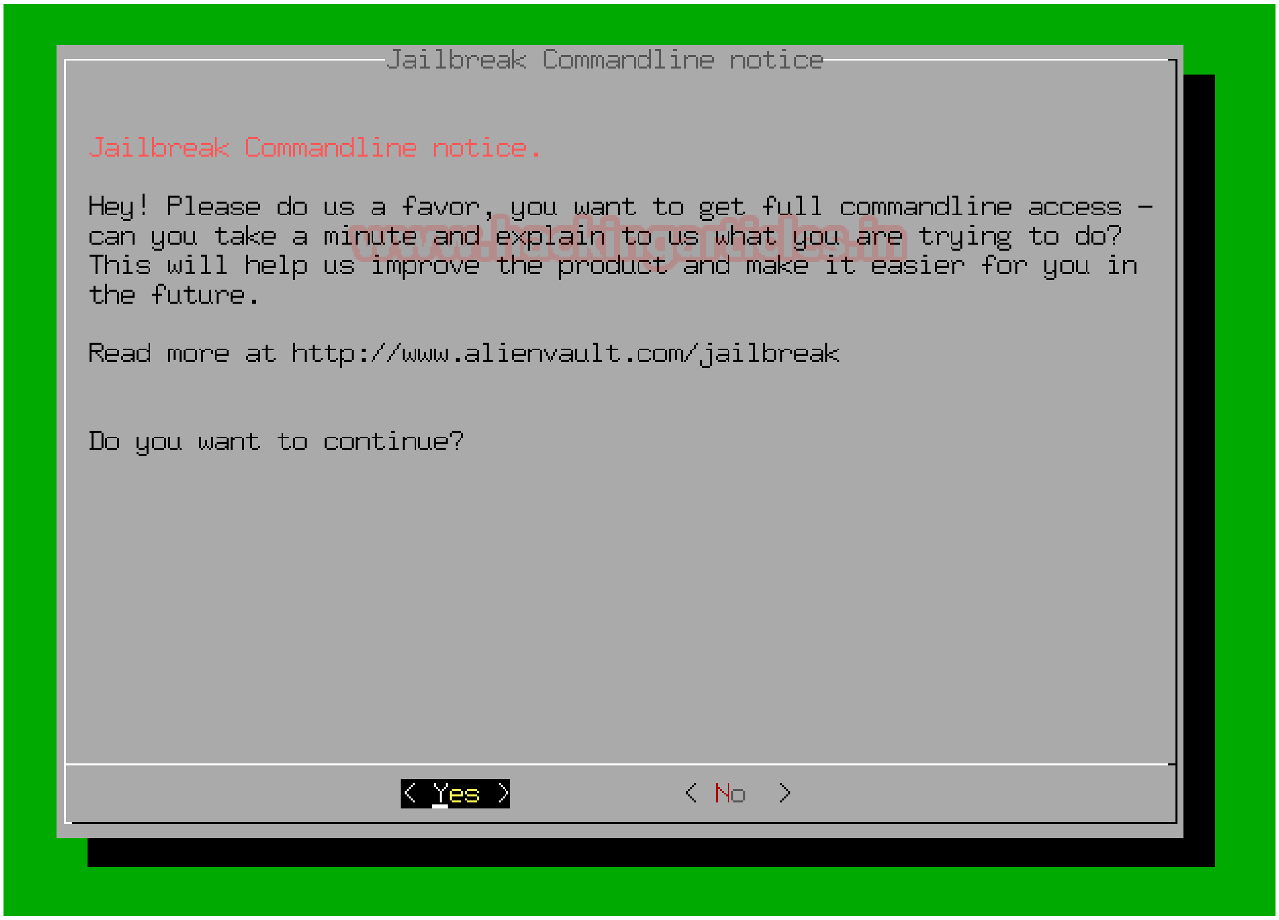
```
root@ignite:/etc/rsyslog.d# /etc/init.d/rsyslog restart
Restarting rsyslog (via systemctl): rsyslog.service.
root@ignite:/etc/rsyslog.d#
```

OSSIM Server

Login to the OSSIM server Jailbreak the server to CLI as shown below



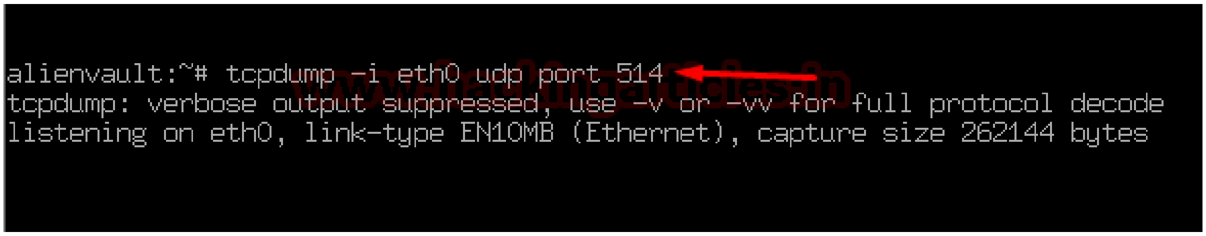
On the next prompt, it will ask you for permission to access the full command line select yes and continue.



```
Jailbreak Commandline notice

Jailbreak Commandline notice.

Hey! Please do us a favor, you want to get full commandline access -
can you take a minute and explain to us what you are trying to do?
This will help us improve the product and make it easier for you in
the future.

Read more at http://www.alienvault.com/jailbreak


Do you want to continue?
```

Here we're using tcpdump on the OSSIM server to see log communications between Ubuntu 20.04 and OSSIM by running tcpdump to capture the logs with the following command:

```
tcpdump -i eth0 udp port 514
```



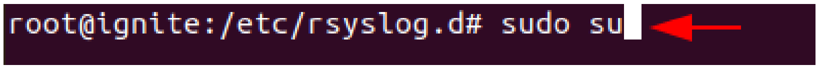
```
alienvault:~# tcpdump -i eth0 udp port 514
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Let's verify whether it is receiving logs from Ubuntu 20.04 server or not

Ubuntu 20.04

In the ubuntu machine, I m switching users by running the following command, and then after we will see the logs of switching users are reflected on the OSSIM server or not.

```
sudo su
```

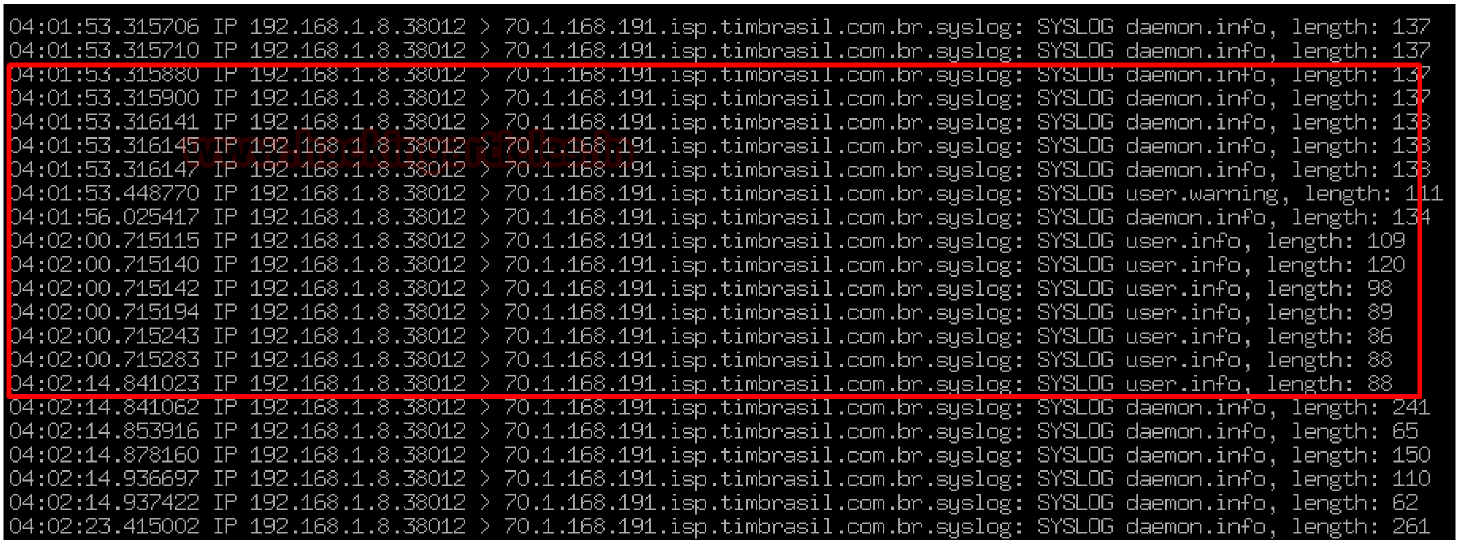


```
root@ignite:/etc/rsyslog.d# sudo su
```

Come back to the OSSIM server

OSSIM Server

Let’s check what happens here …



```
04:01:53.315706 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 137
04:01:53.315710 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 137
04:01:53.315880 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 137
04:01:53.315900 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 137
04:01:53.316141 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 138
04:01:53.316145 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 138
04:01:53.316147 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 138
04:01:53.448770 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG user.warning, length: 111
04:01:56.025417 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 134
04:02:00.715115 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG user.info, length: 109
04:02:00.715140 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG user.info, length: 120
04:02:00.715142 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG user.info, length: 98
04:02:00.715194 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG user.info, length: 89
04:02:00.715243 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG user.info, length: 86
04:02:00.715283 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG user.info, length: 88
04:02:14.841023 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG user.info, length: 88
04:02:14.841062 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 241
04:02:14.853916 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 65
04:02:14.878160 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 150
04:02:14.936697 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 110
04:02:14.937422 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 62
04:02:23.415002 IP 192.168.1.8.38012 > 70.1.168.191.isp.timbrasil.com.br.syslog: SYSLOG daemon.info, length: 261
```

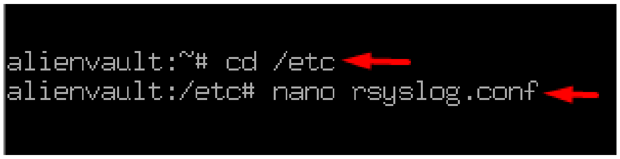
Hurrah !!! as we can see the log from the Ubuntu server has entered into the OSSIM server, then now we will redirect the logs sent to OSSIM into a file.

Now we’re going to **configure the Filtration in the Rsyslog.**

To do this follow the below steps:

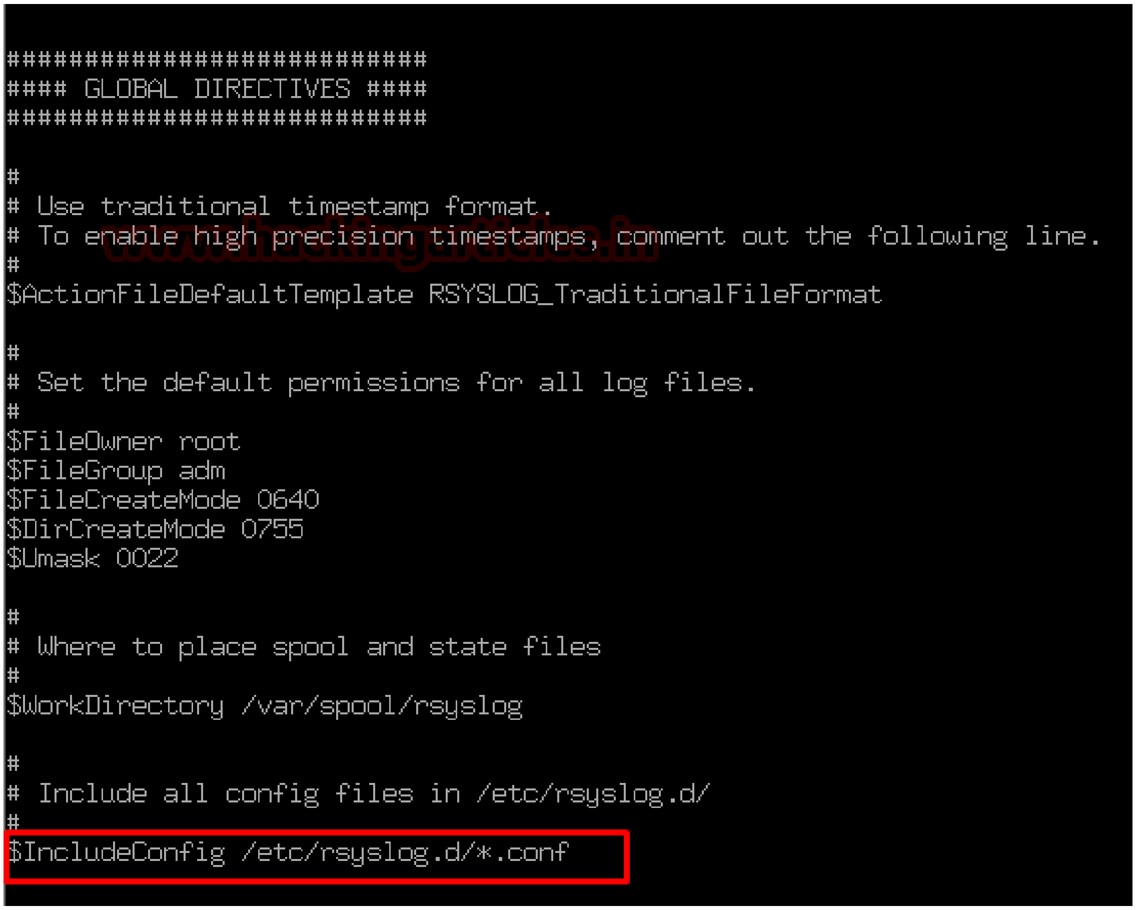
Head towards the **rsyslog.conf** file in the directory **etc.**

```
cd /etc
nano rsyslog.conf
```



```
alienvault:~# cd /etc
alienvault:/etc# nano rsyslog.conf
```

In the section GLOBAL DIRECTIVES, the line **“$IncludeConfig /etc/rsyslog.d/*.conf”** by default it includes the whole config file of the system.

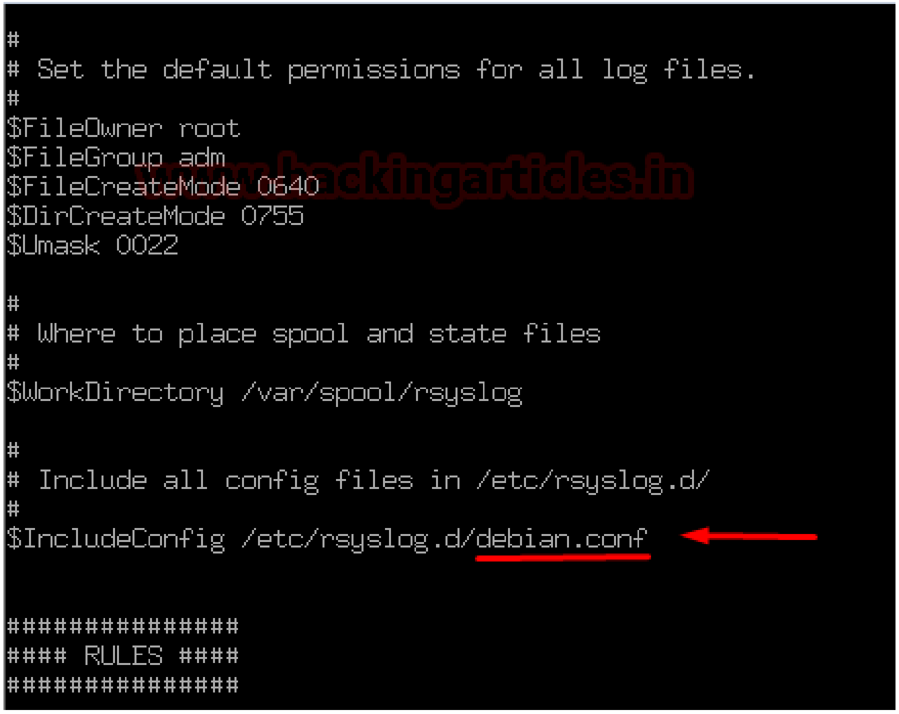


```
############################
#### GLOBAL DIRECTIVES ####
############################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

#
# Set the default permissions for all log files.
#
$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
```

To filter specific rsyslog configurations and logs put some specific name on the place of * to filter it easily as shown below:

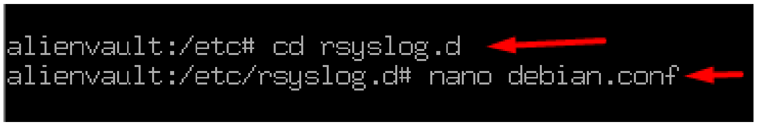
For example:-

```
$IncludeConfig /etc/rsyslog.d/debian.conf
```



```
#
# Set the default permissions for all log files.
#
$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/debian.conf


###############
#### RULES ####
###############
```

Now head towards to directory of rsyslog.d and create a configuration file debian.conf

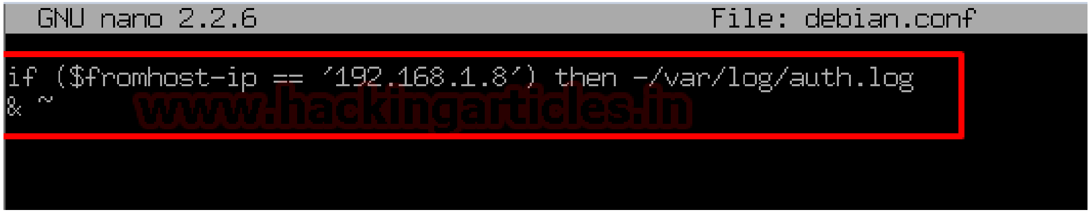


```
alienvault:/etc# cd rsyslog.d
alienvault:/etc/rsyslog.d# nano debian.conf
```

And enter the following rule into it:

```
If $fromhost-ip == ‘192.168.1.8’ then -/var/log/auth.log
&~
```

Then save and exit as shown below

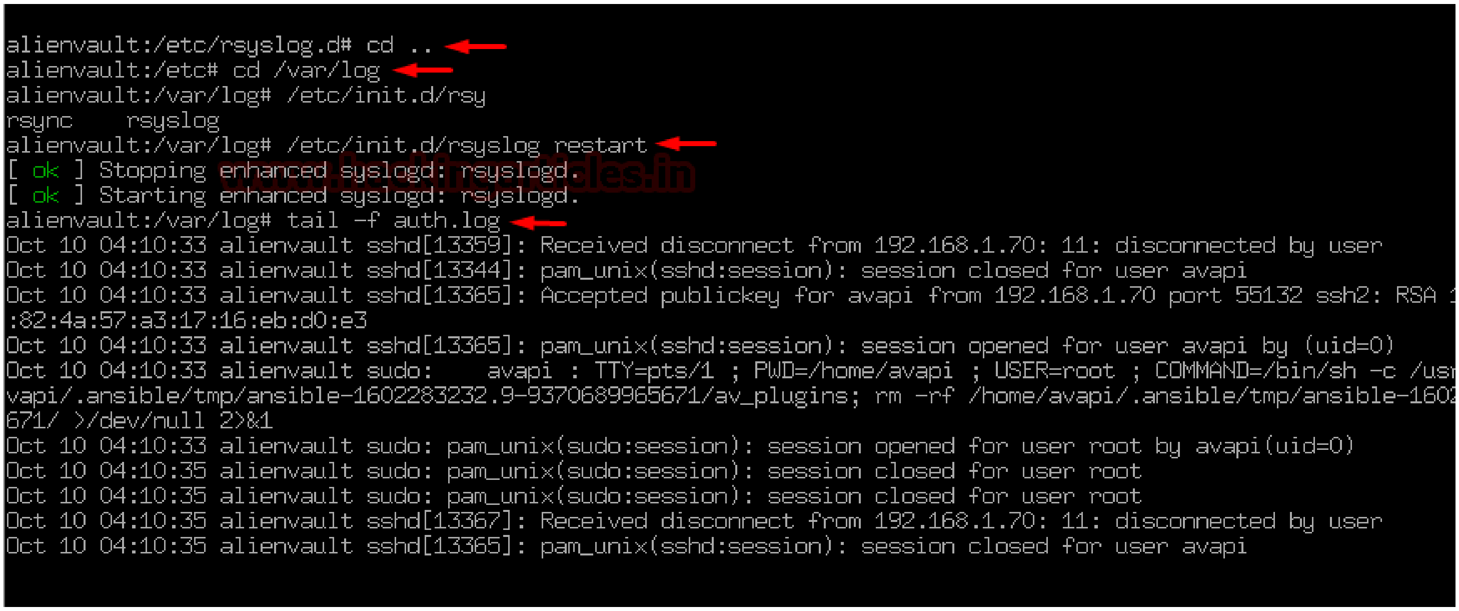


```
  GNU nano 2.2.6                              File: debian.conf

if ($fromhost-ip == '192.168.1.8') then -/var/log/auth.log
& ~
```

Now we check that the logs of the ubuntu server are inserted correctly in auth.log or not.

Before we do rsyslog restart and then follow the below steps:

```
cd /var/log
/etc/init.d/rsyslog restart
tail -f auth.log
```



```
alienvault:/etc/rsyslog.d# cd ..
alienvault:/etc# cd /var/log
alienvault:/var/log# /etc/init.d/rsy
rsync    rsyslog
alienvault:/var/log# /etc/init.d/rsyslog restart
[ ok ] Stopping enhanced syslogd: rsyslogd.
[ ok ] Starting enhanced syslogd: rsyslogd.
alienvault:/var/log# tail -f auth.log
Oct 10 04:10:33 alienvault sshd[13359]: Received disconnect from 192.168.1.70: 11: disconnected by user
Oct 10 04:10:33 alienvault sshd[13344]: pam_unix(sshd:session): session closed for user avapi
Oct 10 04:10:33 alienvault sshd[13365]: Accepted publickey for avapi from 192.168.1.70 port 55132 ssh2: RSA 1
:82:4a:57:a3:17:16:eb:d0:e3
Oct 10 04:10:33 alienvault sshd[13365]: pam_unix(sshd:session): session opened for user avapi by (uid=0)
Oct 10 04:10:33 alienvault sudo:    avapi : TTY=pts/1 ; PWD=/home/avapi ; USER=root ; COMMAND=/bin/sh -c /usr
vapi/.ansible/tmp/ansible-1602283232.9-9370689965671/av_plugins; rm -rf /home/avapi/.ansible/tmp/ansible-1602
671/ >/dev/null 2>&1
Oct 10 04:10:33 alienvault sudo: pam_unix(sudo:session): session opened for user root by avapi(uid=0)
Oct 10 04:10:35 alienvault sudo: pam_unix(sudo:session): session closed for user root
Oct 10 04:10:35 alienvault sudo: pam_unix(sudo:session): session closed for user root
Oct 10 04:10:35 alienvault sshd[13367]: Received disconnect from 192.168.1.70: 11: disconnected by user
Oct 10 04:10:35 alienvault sshd[13365]: pam_unix(sshd:session): session closed for user avapi
```

As we can see logs are started coming from the ubuntu server ?

Now we move on to the AlienVault part

OSSIM needs a plug-in t to connect any data source to the server. Plugins have XML based configuration.

The plugins have two elements: **cfg and SQL**

Let’s go to configure **cfg**

To do this head towards the directory /etc/ossim/agent/plugins

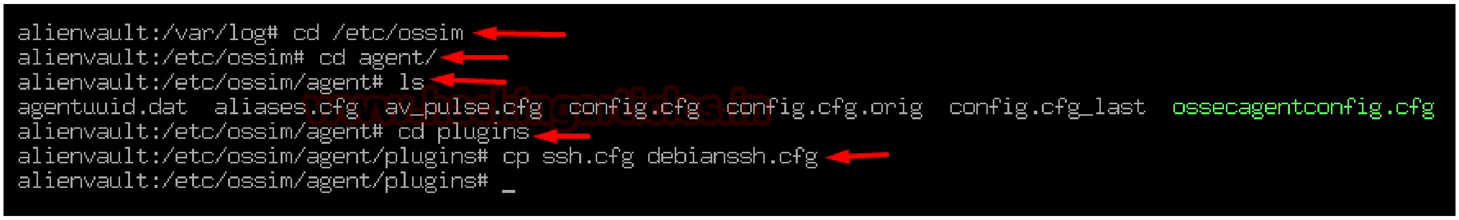
```
cd /etc/ossim
cd agent/
cd plugins/
```

in the directory of plugins, there are lots of plugins available that can be activated in OSSIM

we went on to modify one by hand **for example SSH**

To do this run the following command:

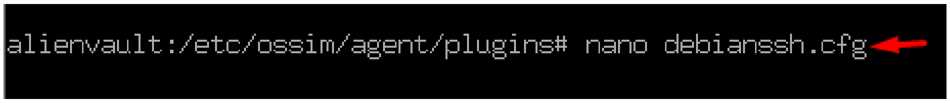
```
cp ssh.cfg debianssh.cfg
```



```
alienvault:/var/log# cd /etc/ossim
alienvault:/etc/ossim# cd agent/
alienvault:/etc/ossim/agent# ls
agentuuid.dat  aliases.cfg  av_pulse.cfg  config.cfg  config.cfg.orig  config.cfg_last  ossecagentconfig.cfg
alienvault:/etc/ossim/agent# cd plugins
alienvault:/etc/ossim/agent/plugins# cp ssh.cfg debianssh.cfg
alienvault:/etc/ossim/agent/plugins# _
```

Then after open the debianssh.cfg configuration file.

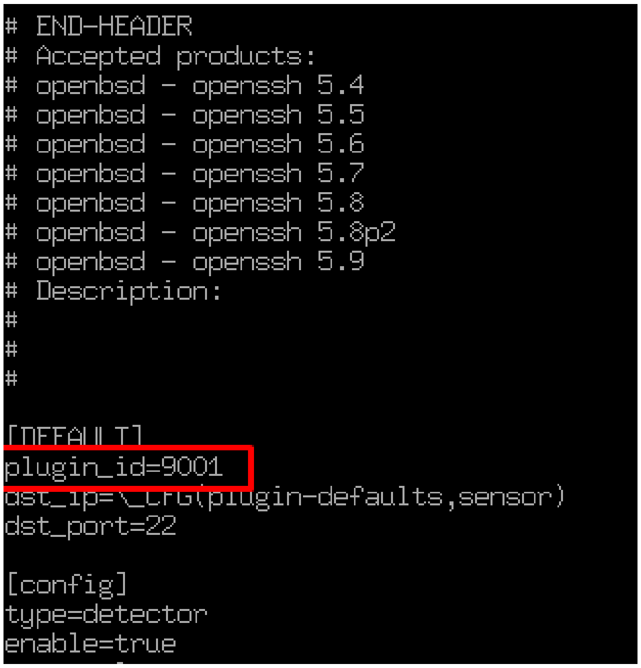
```
nano debiannssh.cfg
```



```
alienvault:/etc/ossim/agent/plugins# nano debianssh.cfg
```

And change the plugin id with your desired no. to make it identifiable for the further process.

Here I'm replacing plugin id 4003 to 9001 as shown below:

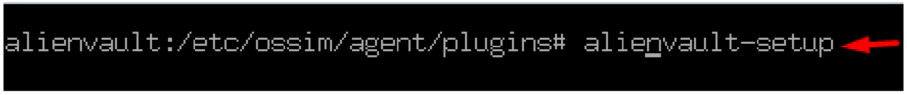


```
# END-HEADER
# Accepted products:
# openbsd - openssh 5.4
# openbsd - openssh 5.5
# openbsd - openssh 5.6
# openbsd - openssh 5.7
# openbsd - openssh 5.8
# openbsd - openssh 5.8p2
# openbsd - openssh 5.9
# Description:
#
#
#

[DEFAULT]
plugin_id=9001
dst_ip=\_CFG(plugin-defaults,sensor)
dst_port=22

[config]
type=detector
enable=true
```

Now we can activate the plugin

Come back to AlienVault setup by entering the following command:

```
alienvault-setup
```

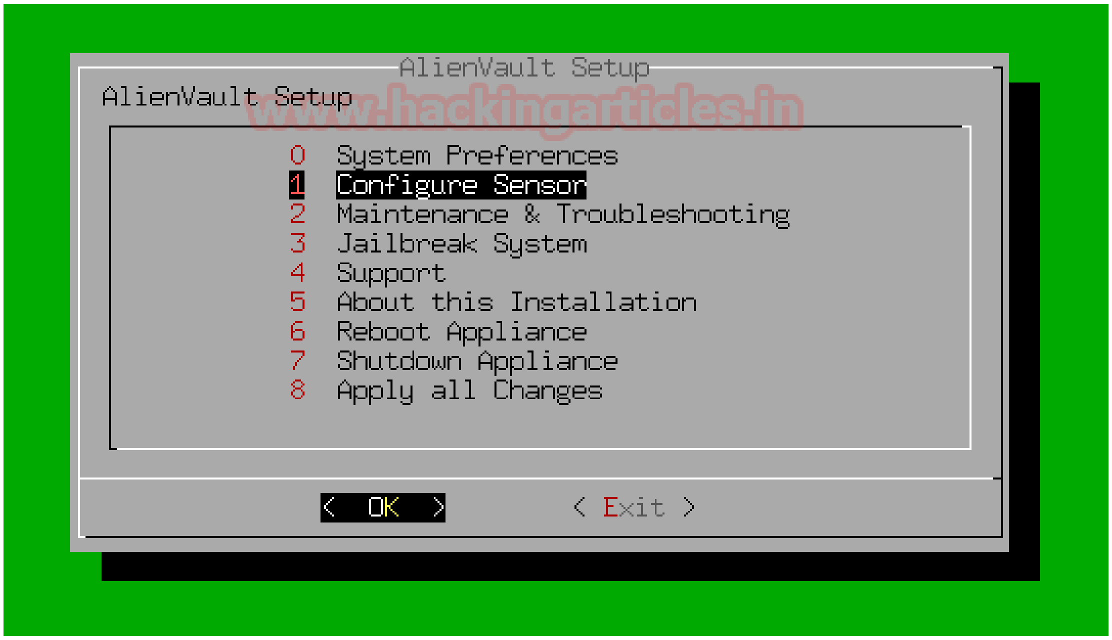


```
alienvault:/etc/ossim/agent/plugins# alienvault-setup
```

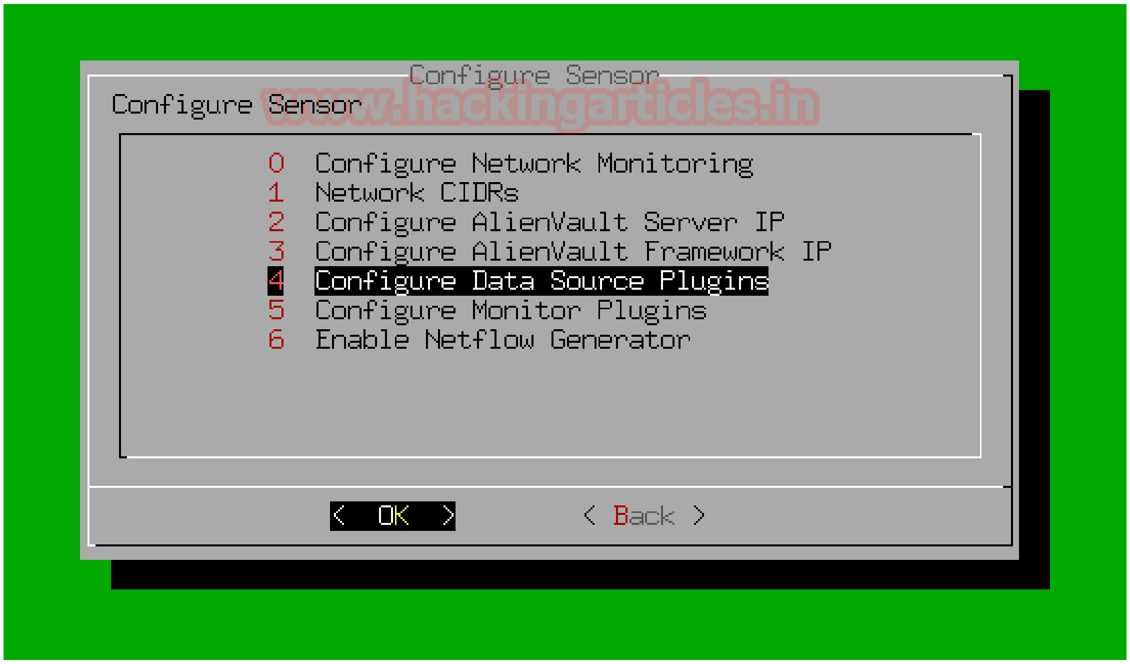
And then configure the sensor by the below steps:

Select Configure Sensor > Configure Data Source Plugins > debianssh

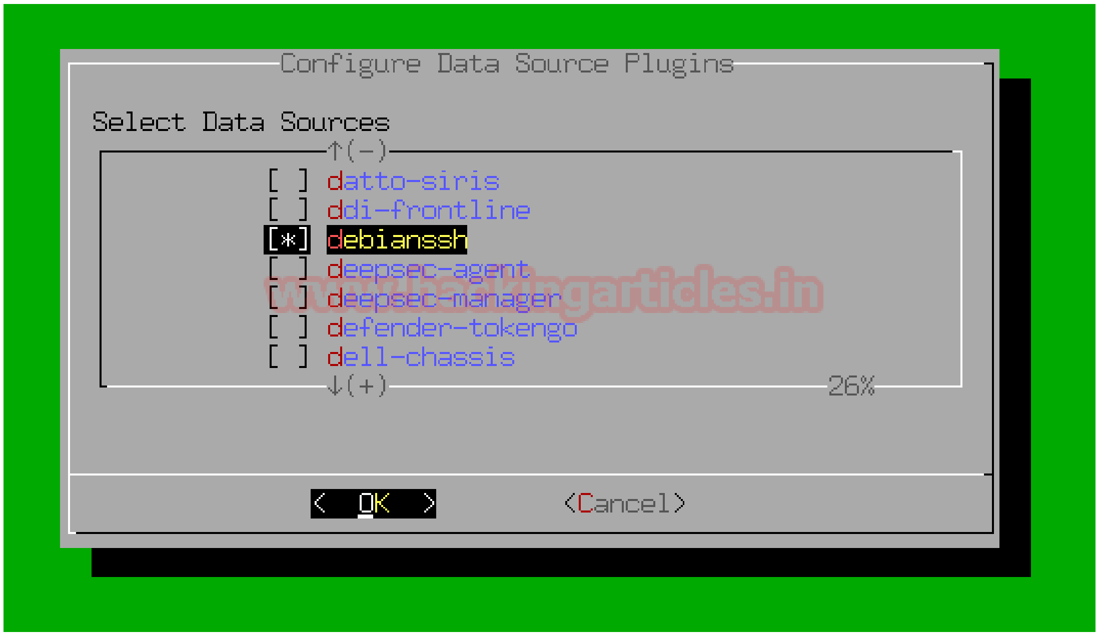
Select Configure sensor



Select Configure Data Source Plugins

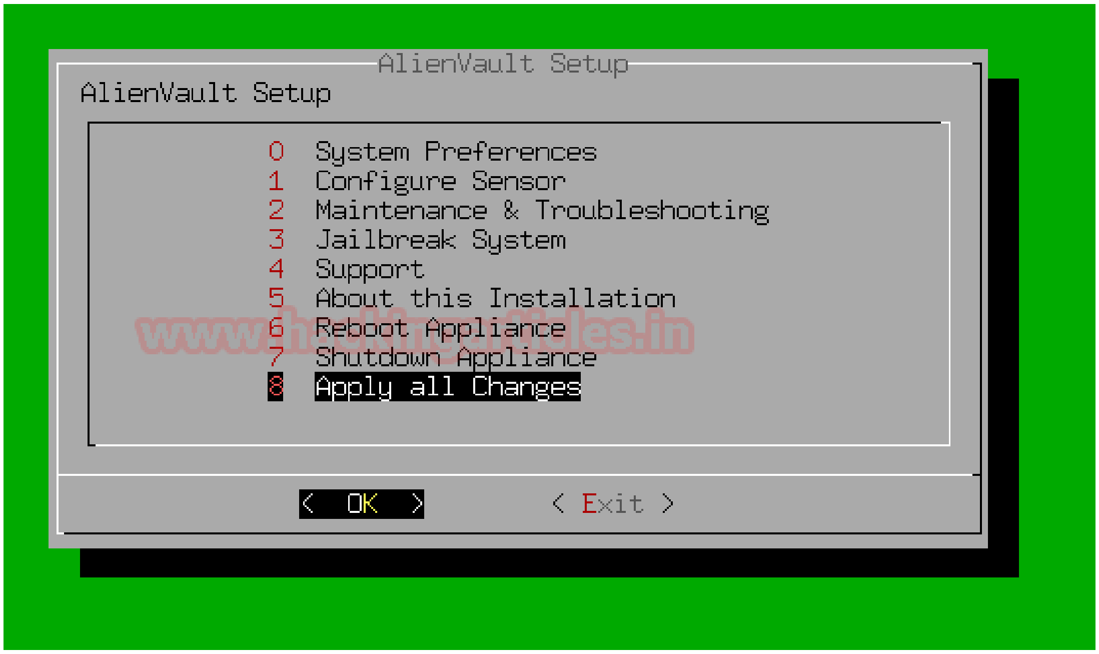

Configure Sensor
Configure Sensor
www.hackingarticles.in
0 Configure Network Monitoring
1 Network CIDRs
2 Configure AlienVault Server IP
3 Configure AlienVault Framework IP
4 Configure Data Source Plugins
5 Configure Monitor Plugins
6 Enable Netflow Generator
< OK >
< Back >

In the previous steps, we modified an SSH plugin into **debianssh** plugin. Select it in the list of plugins by pressing spacebar as shown below



```
Configure Data Source Plugins

Select Data Sources
            ↑(-)
        [ ] datto-siris
        [ ] ddi-frontline
        [*] debianssh
        [ ] deepsec-agent
        [ ] deepsec-manager
        [ ] defender-tokengo
        [ ] dell-chassis
            ↓(+)                     26%

        <  OK  >        <Cancel>
```

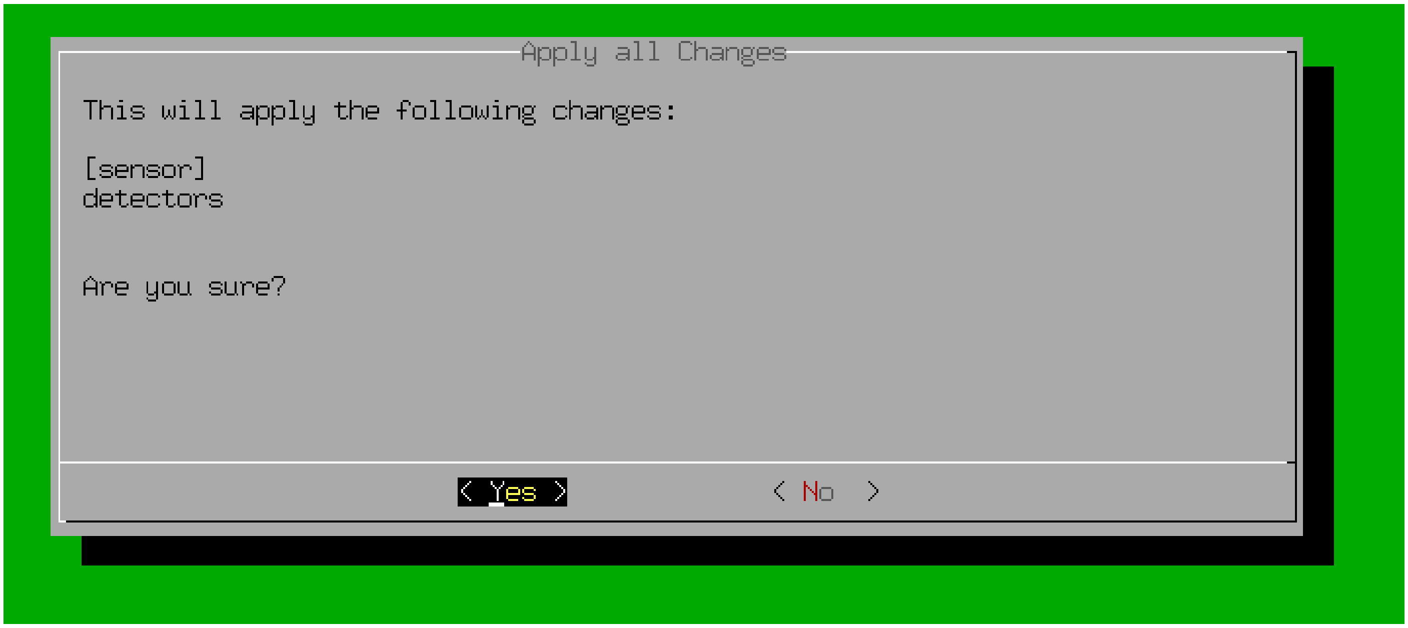
And then come back to AlienVault Setup by selecting back option and then **Apply All Changes**



```
AlienVault Setup
AlienVault Setup

        0  System Preferences
        1  Configure Sensor
        2  Maintenance & Troubleshooting
        3  Jailbreak System
        4  Support
        5  About this Installation
        6  Reboot Appliance
        7  Shutdown Appliance
        8  Apply all Changes

        <  OK  >        <  Exit  >
```

At last, it will ask for your permission to apply all changes

Select **yes** and then **continue**

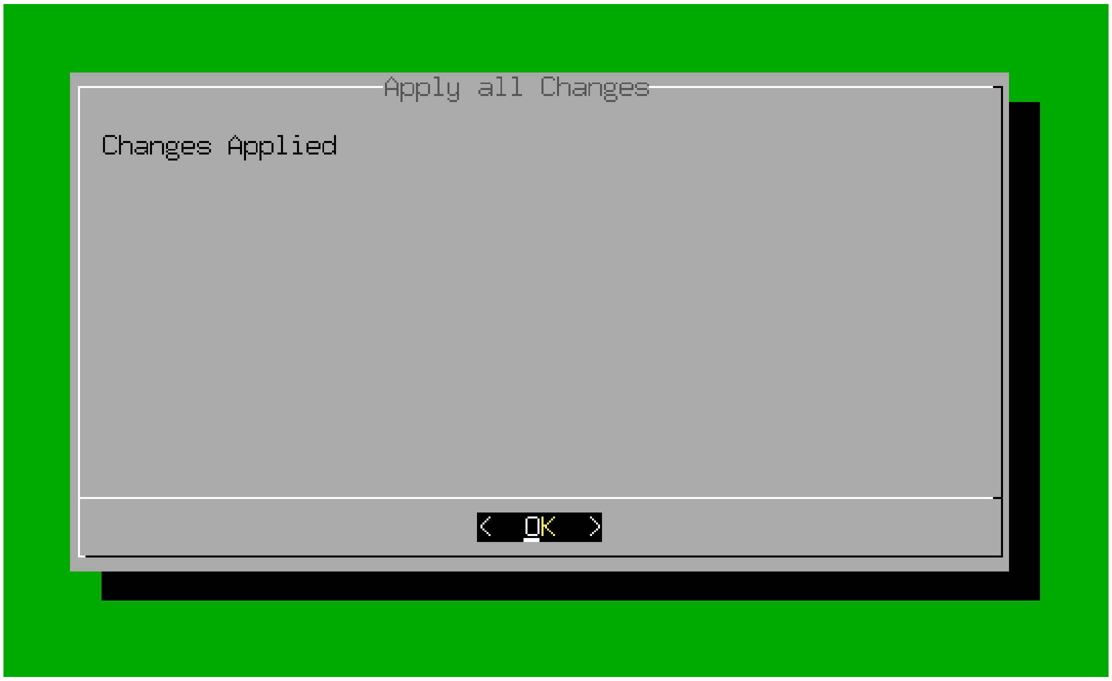

Apply all Changes

This will apply the following changes:

[sensor]
detectors

Are you sure?

On the next prompt, it will show you changes applied


Apply all Changes

Changes Applied

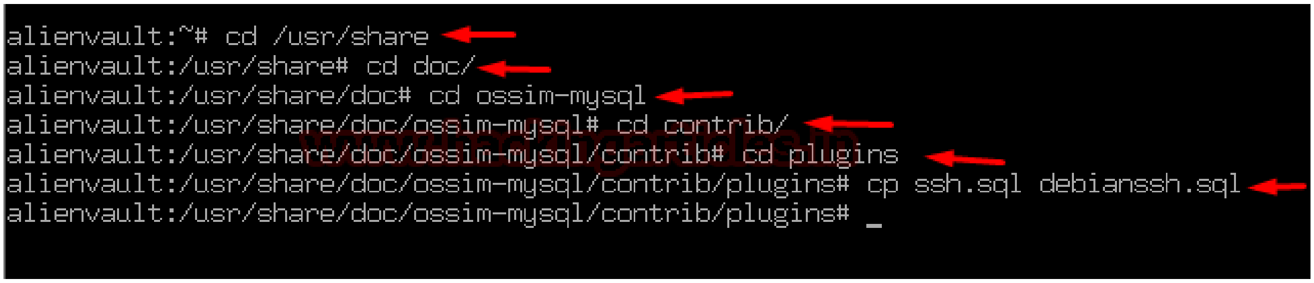
Let’s go to configure the SQL part of the plugin.

Head towards to the directory of /usr/share/doc/ossim-mysql/contrib/plugins by entering the following command

```
cd /usr/share
cd /doc
cd /ossim-mysql
cd /contrib
cd /plugins
```

by running command ls you can see the examples of sql plugins we’re going to copy the ssh.sql to debianssh.sql by running the following command:

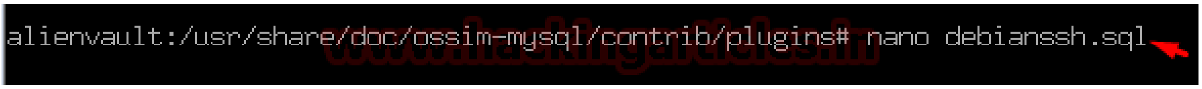
```
cp ssh.sql debianssh.sql
```



```
alienvault:~# cd /usr/share
alienvault:/usr/share# cd doc/
alienvault:/usr/share/doc# cd ossim-mysql
alienvault:/usr/share/doc/ossim-mysql# cd contrib/
alienvault:/usr/share/doc/ossim-mysql/contrib# cd plugins
alienvault:/usr/share/doc/ossim-mysql/contrib/plugins# cp ssh.sql debianssh.sql
alienvault:/usr/share/doc/ossim-mysql/contrib/plugins# _
```

Open the debianssh.sql file

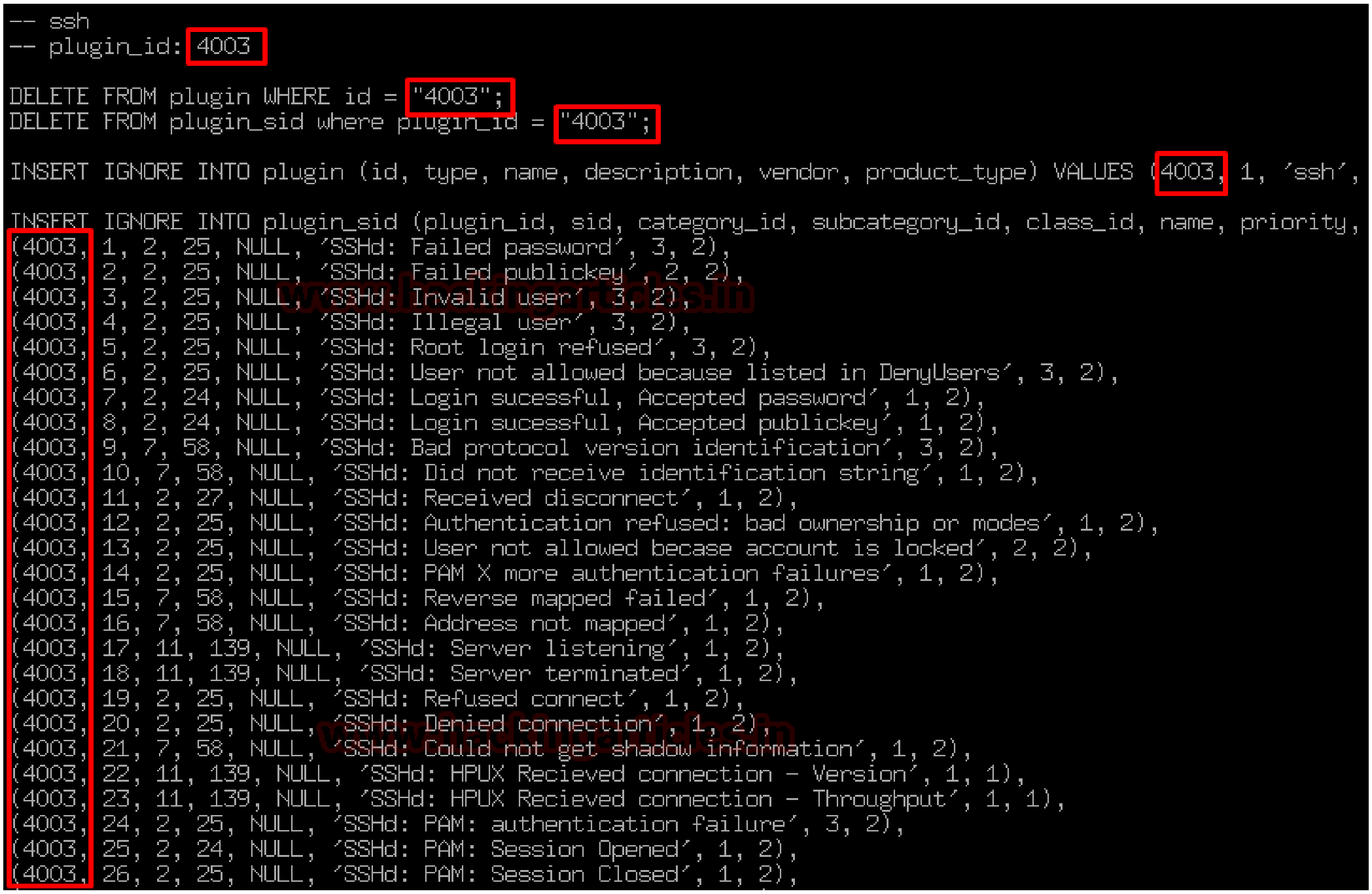
```
nano debianssh.sql
```



```
alienvault:/usr/share/doc/ossim-mysql/contrib/plugins# nano debianssh.sql
```

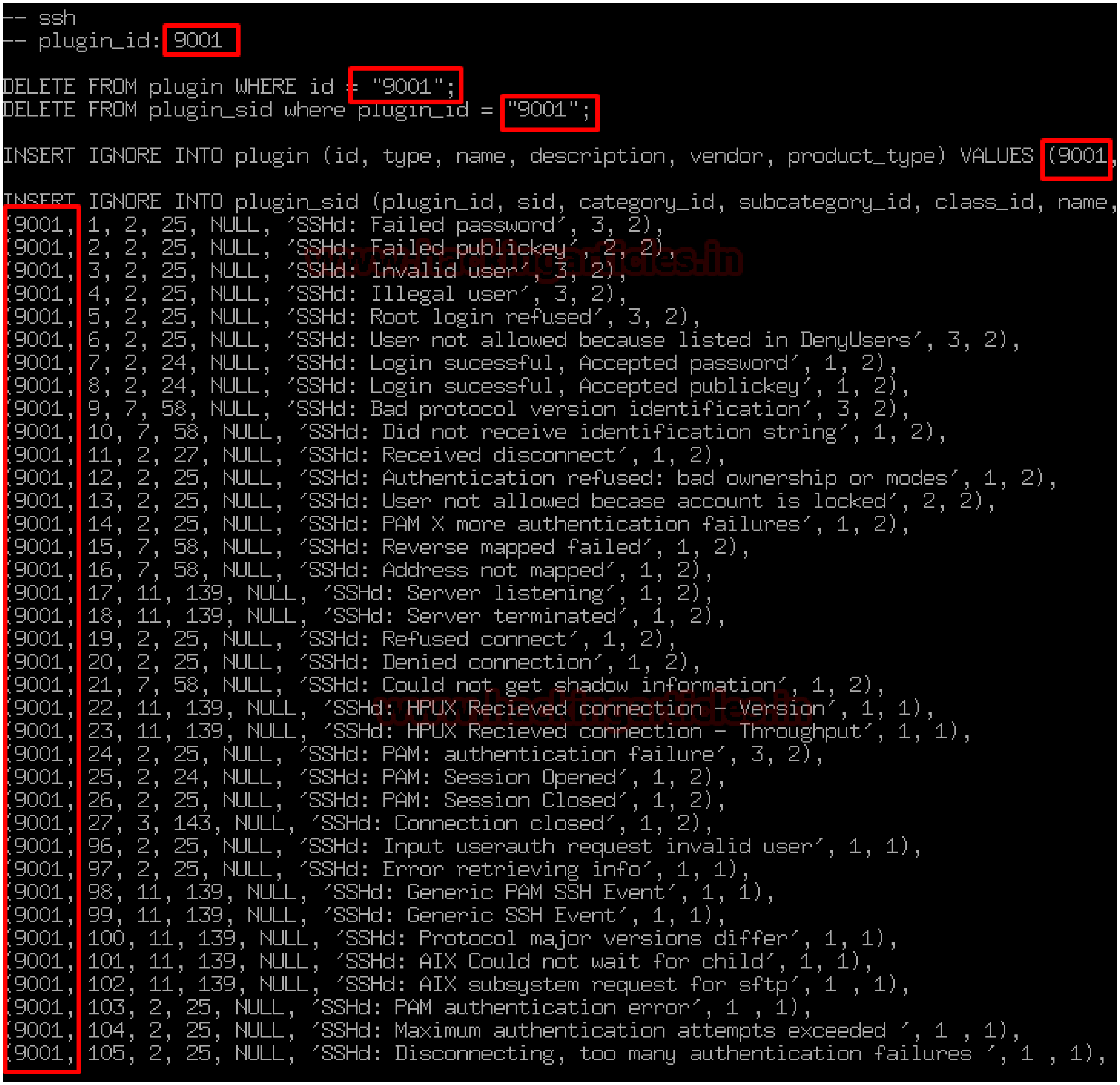
Let’s do some modifications in the configuration file so that it can match the plugin.cfg to the SQL database.

The configuration looks like similar as shown below



```
-- ssh
-- plugin_id: 4003

DELETE FROM plugin WHERE id = "4003";
DELETE FROM plugin_sid where plugin_id = "4003";

INSERT IGNORE INTO plugin (id, type, name, description, vendor, product_type) VALUES (4003, 1, 'ssh',

INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, subcategory_id, class_id, name, priority,
(4003, 1, 2, 25, NULL, 'SSHd: Failed password', 3, 2),
(4003, 2, 2, 25, NULL, 'SSHd: Failed publickey', 2, 2),
(4003, 3, 2, 25, NULL, 'SSHd: Invalid user', 3, 2),
(4003, 4, 2, 25, NULL, 'SSHd: Illegal user', 3, 2),
(4003, 5, 2, 25, NULL, 'SSHd: Root login refused', 3, 2),
(4003, 6, 2, 25, NULL, 'SSHd: User not allowed because listed in DenyUsers', 3, 2),
(4003, 7, 2, 24, NULL, 'SSHd: Login sucessful, Accepted password', 1, 2),
(4003, 8, 2, 24, NULL, 'SSHd: Login sucessful, Accepted publickey', 1, 2),
(4003, 9, 7, 58, NULL, 'SSHd: Bad protocol version identification', 3, 2),
(4003, 10, 7, 58, NULL, 'SSHd: Did not receive identification string', 1, 2),
(4003, 11, 2, 27, NULL, 'SSHd: Received disconnect', 1, 2),
(4003, 12, 2, 25, NULL, 'SSHd: Authentication refused: bad ownership or modes', 1, 2),
(4003, 13, 2, 25, NULL, 'SSHd: User not allowed becase account is locked', 2, 2),
(4003, 14, 2, 25, NULL, 'SSHd: PAM X more authentication failures', 1, 2),
(4003, 15, 7, 58, NULL, 'SSHd: Reverse mapped failed', 1, 2),
(4003, 16, 7, 58, NULL, 'SSHd: Address not mapped', 1, 2),
(4003, 17, 11, 139, NULL, 'SSHd: Server listening', 1, 2),
(4003, 18, 11, 139, NULL, 'SSHd: Server terminated', 1, 2),
(4003, 19, 2, 25, NULL, 'SSHd: Refused connect', 1, 2),
(4003, 20, 2, 25, NULL, 'SSHd: Denied connection', 1, 2),
(4003, 21, 7, 58, NULL, 'SSHd: Could not get shadow information', 1, 2),
(4003, 22, 11, 139, NULL, 'SSHd: HPUX Recieved connection - Version', 1, 1),
(4003, 23, 11, 139, NULL, 'SSHd: HPUX Recieved connection - Throughput', 1, 1),
(4003, 24, 2, 25, NULL, 'SSHd: PAM: authentication failure', 3, 2),
(4003, 25, 2, 24, NULL, 'SSHd: PAM: Session Opened', 1, 2),
(4003, 26, 2, 25, NULL, 'SSHd: PAM: Session Closed', 1, 2),
```

Change the plugin id 4001 to 9001 or somewhat the value of no. that you designated in the upper section as shown below:



```
-- ssh
-- plugin_id: 9001

DELETE FROM plugin WHERE id = "9001";
DELETE FROM plugin_sid where plugin_id = "9001";

INSERT IGNORE INTO plugin (id, type, name, description, vendor, product_type) VALUES (9001,

INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, subcategory_id, class_id, name,
(9001, 1, 2, 25, NULL, 'SSHd: Failed password', 3, 2),
(9001, 2, 2, 25, NULL, 'SSHd: Failed publickey', 2, 2),
(9001, 3, 2, 25, NULL, 'SSHd: Invalid user', 3, 2),
(9001, 4, 2, 25, NULL, 'SSHd: Illegal user', 3, 2),
(9001, 5, 2, 25, NULL, 'SSHd: Root login refused', 3, 2),
(9001, 6, 2, 25, NULL, 'SSHd: User not allowed because listed in DenyUsers', 3, 2),
(9001, 7, 2, 24, NULL, 'SSHd: Login sucessful, Accepted password', 1, 2),
(9001, 8, 2, 24, NULL, 'SSHd: Login sucessful, Accepted publickey', 1, 2),
(9001, 9, 7, 58, NULL, 'SSHd: Bad protocol version identification', 3, 2),
(9001, 10, 7, 58, NULL, 'SSHd: Did not receive identification string', 1, 2),
(9001, 11, 2, 27, NULL, 'SSHd: Received disconnect', 1, 2),
(9001, 12, 2, 25, NULL, 'SSHd: Authentication refused: bad ownership or modes', 1, 2),
(9001, 13, 2, 25, NULL, 'SSHd: User not allowed becase account is locked', 2, 2),
(9001, 14, 2, 25, NULL, 'SSHd: PAM X more authentication failures', 1, 2),
(9001, 15, 7, 58, NULL, 'SSHd: Reverse mapped failed', 1, 2),
(9001, 16, 7, 58, NULL, 'SSHd: Address not mapped', 1, 2),
(9001, 17, 11, 139, NULL, 'SSHd: Server listening', 1, 2),
(9001, 18, 11, 139, NULL, 'SSHd: Server terminated', 1, 2),
(9001, 19, 2, 25, NULL, 'SSHd: Refused connect', 1, 2),
(9001, 20, 2, 25, NULL, 'SSHd: Denied connection', 1, 2),
(9001, 21, 7, 58, NULL, 'SSHd: Could not get shadow information', 1, 2),
(9001, 22, 11, 139, NULL, 'SSHd: HPUX Recieved connection - Version', 1, 1),
(9001, 23, 11, 139, NULL, 'SSHd: HPUX Recieved connection - Throughput', 1, 1),
(9001, 24, 2, 25, NULL, 'SSHd: PAM: authentication failure', 3, 2),
(9001, 25, 2, 24, NULL, 'SSHd: PAM: Session Opened', 1, 2),
(9001, 26, 2, 25, NULL, 'SSHd: PAM: Session Closed', 1, 2),
(9001, 27, 3, 143, NULL, 'SSHd: Connection closed', 1, 2),
(9001, 96, 2, 25, NULL, 'SSHd: Input userauth request invalid user', 1, 1),
(9001, 97, 2, 25, NULL, 'SSHd: Error retrieving info', 1, 1),
(9001, 98, 11, 139, NULL, 'SSHd: Generic PAM SSH Event', 1, 1),
(9001, 99, 11, 139, NULL, 'SSHd: Generic SSH Event', 1, 1),
(9001, 100, 11, 139, NULL, 'SSHd: Protocol major versions differ', 1, 1),
(9001, 101, 11, 139, NULL, 'SSHd: AIX Could not wait for child', 1, 1),
(9001, 102, 11, 139, NULL, 'SSHd: AIX subsystem request for sftp', 1 , 1),
(9001, 103, 2, 25, NULL, 'SSHd: PAM authentication error', 1 , 1),
(9001, 104, 2, 25, NULL, 'SSHd: Maximum authentication attempts exceeded ', 1 , 1),
(9001, 105, 2, 25, NULL, 'SSHd: Disconnecting, too many authentication failures ', 1 , 1),
```

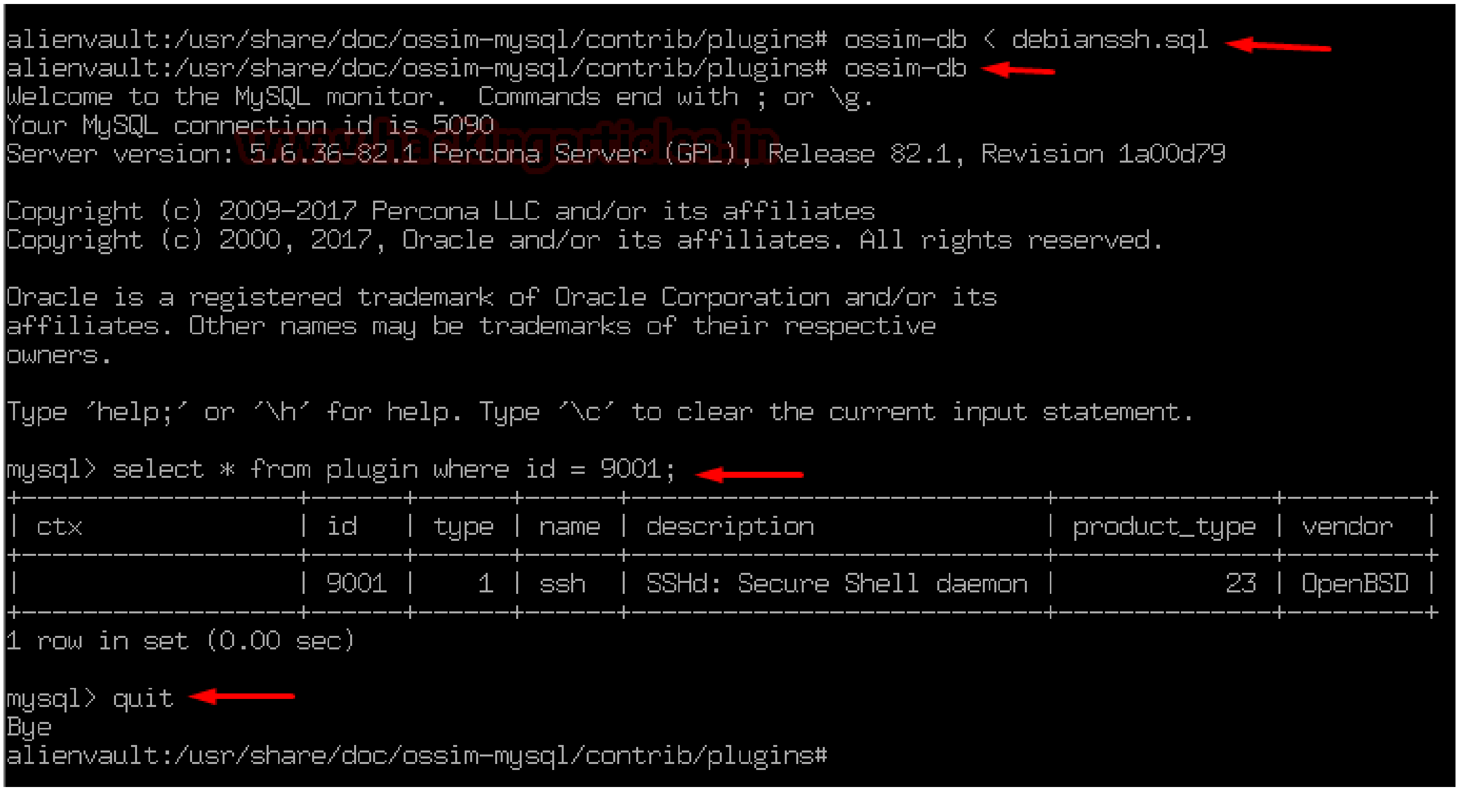
As you can see this configuration file contains a predefined database of SSH logs so that if any suspicious SSH activity or request comes to the Ubuntu server it can match with that request.

And then Save and exit from the file.

Let's put it into the action and activate the database be reconfiguring it.

To do this enter the following command:

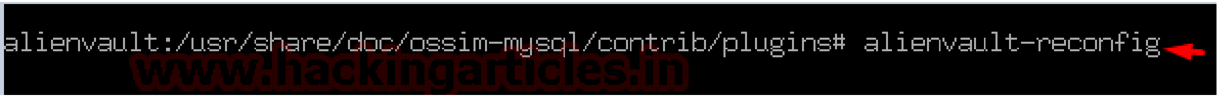
```
ossim-db < debianssh.sql
ossim-db
select * from plugin where id = 9001;
quit
```



```
alienvault:/usr/share/doc/ossim-mysql/contrib/plugins# ossim-db < debianssh.sql
alienvault:/usr/share/doc/ossim-mysql/contrib/plugins# ossim-db
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5090
Server version: 5.6.36-82.1 Percona Server (GPL), Release 82.1, Revision 1a00d79

Copyright (c) 2009-2017 Percona LLC and/or its affiliates
Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from plugin where id = 9001;
+--------------------+------+------+------+---------------------------+--------------+---------+
| ctx                | id   | type | name | description               | product_type | vendor  |
+--------------------+------+------+------+---------------------------+--------------+---------+
|                    | 9001 |    1 | ssh  | SSHd: Secure Shell daemon |           23 | OpenBSD |
+--------------------+------+------+------+---------------------------+--------------+---------+
1 row in set (0.00 sec)

mysql> quit
Bye
alienvault:/usr/share/doc/ossim-mysql/contrib/plugins#
```

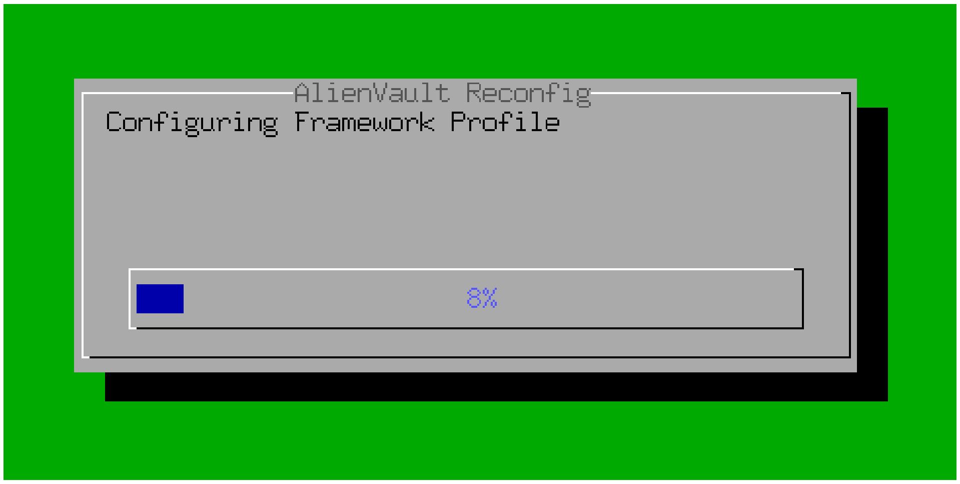
And at last reconfig the AlienVault OSSIM server by entering the following command:

```
alienvault-reconfig
```



```
alienvault:/usr/share/doc/ossim-mysql/contrib/plugins# alienvault-reconfig
```

On the next screen, it will start reconfiguring the server



```
AlienVault Reconfig
Configuring Framework Profile

8%
```

If you are seeing this then congratulations…!!!

You successfully integrated Rsyslog and SSH plugin to the AlienVault OSSIMa server.

Hold tight! this is not enough…..

Have patience ?

In this article, we explained the integration and configuration process of Rsyslog and SSH plugin to AlienVault OSSIM.

In the next article, our focus will be on the configuration and installation of OSSEc Agents that send logs to **AlienVault Server.**

OSSEC is an open-source Host Intrusion Detection System (HIDS) that runs across multiple OS platforms such as Windows, Linux, Solaris. Mac …etc.