Allien Vault OSSIM Custom Plugin Oluşturmak

Alien Vault OSSIM üzerinde özel plugin yazmak için aşağıdaki adımlar takip edilir.

1- Plugin için konfigurasyon dosyası oluşturulur.

/etc/ossim/agent/plugins/elastichoney.cfg

Not:

a- Regex yazımı için regex101.com sitesi kullanılabilir.

b- Regex yazarken değeri boş gelen bir alan var ise null|değer şeklinde tanımlanmalıdır.

```
# Alienvault plugin
# Author: Fatih usta <fatihusta@labrisnetworks.com>
# Plugin elastichoney id:91111 version: 0.0.1
# Last modification: 2018-10-09 10:15
#
# Plugin Selection Info:
# elastichoney:-
#
# END-HEADER
#
# Description:
#   elastichoney
#
#
#
#

[DEFAULT]
plugin_id=91111

[config]
type=detector
enable=yes

source=log
location=/var/log/elastichoney.log

create_file=false

process=
start=no
stop=no
startup=
shutdown=

[translation]
attack=1
recon=2


#Oct 22 13:47:54 ahtapot elastichoney {"source":"10.0.3.254","@timestamp":"2018-10-22
16:47:55.585121988","url":"10.0.3.24:9200/_search?pretty","method":"POST","form":"pretty=&%7B%22script_fields%22%3A+
%7B%22myscript%22%3A+%7B%22script%22%3A+%22java.lang.Math.class.forName%28%5C%22java.lang.Runtime%5C%22%2
9%22%7D%7D%7D=","payload":"","payloadCommand":"","payloadResource":"","payloadMd5":"","payloadBinary":"","headers"
:{"user_agent":"curl/7.52.1","host":"10.0.3.24:9200","content_type":"application/x-www-form-urlencoded","accept_language"
```

:""},"type":"attack","honeypot":"10.0.3.24"}

[0001 - elastichoney]
event_type=event
regexp='\w+\s\d+\s\d+:\d+:\d+\s(?P<device>\w+)\s(?P<sensor>\w+)\s{"\w+":"(?P<source>\d{1,3}.{1,3}.{1,3}.{1,3})","@\w+":"(?P<date>\d+-\d+-\d+\s\d+:\d+:\d+).\d+","\w+":(?P<url>".*?"),"\w+":"(?P<method>\w+)","\w+":(?P<form>".*?"),"\w+":(?P<payload>"null|.*?"),"\w+":(?P<payload_command>"null|.*?"),"\w+":(?P<peyload_resource>"null|.*?"),"\w+":(?P<payload_md5>"null|.*?"),"\w+":(?P<payload_binary>"null|.*?"),"\w+":{"\w+":(?P<user_agent>"null|.*?"),"\w+":"(?P<host>\d{1,3}.{1,3}.{1,3}.{1,3}):(?P<dst_port>\d+)","\w+":(?P<content_type>".*?"),"\w+":(?P<accept_language>"null|.*?")},"\w+":"(?P<type>\w+)","\w+":"(?P<destination>\d{1,3}.{1,3}.{1,3}.{1,3})"}'
date={$date}
device={$device}
plugin_sid={translate($type)}
src_ip={$source}
dst_ip={$destination}
dst_port={$dst_port}
userdata1={$url}
userdata2={$method}
userdata3={$form}
userdata4={$payload}
userdata5={$payload_command}
userdata6={$payload_resource}
userdata7={$payload_md5}
userdata8={$payload_binary}
userdata9=headers: Host: {$host}:{$dst_port}, User-Agent: ${$user_agent}, Content-Type: {$content_type}, Accept-Language:

```
{$accept_language}
```

Plugin Sid Nedir?: Gelen logun veri tabanında karşılığı olan kaydın ID'sidir. Bu sid numarasına göre veri tabanı şekillendirilmeli ve config dosyasındaki translation kısmı buna göre düzenlenmelidir.
Translate Bölümünün Mantığı: Gelen log içinde type'a göre plugin_sid numarasına otomatik çevirip veri tabanı ile eşleştirip alarm üreten bölümdür.

2- Plugin için veritabanı dosyası oluştur ve ossim-db aracını kullanarak veritabanına dahil edilir.

/usr/share/doc/ossim-mysql/contrib/plugins/elastichoney.sql

```
-- elastichoney
-- plugin_id: 91111
--
SET @pluginid = 91111;
SET @type = 1;
SET @pluginname = 'elastichoney';
SET @desc = 'Elastichoney: Elastic Search Honeypot (CVE-2015-1427)';
SET @product_type = 11;
SET @vendor = NULL;
DELETE FROM plugin WHERE id = @pluginid;
DELETE FROM plugin_sid where plugin_id = @pluginid;
-- id    | type | name     | description                | product_type | vendor
INSERT IGNORE INTO plugin (id, type, name, description, product_type, vendor) VALUES (@pluginid, @type, @pluginname,
@desc, @product_type, @vendor);
-- plugin_id | sid       | class_id | reliability | priority | name                    | aro    | subcategory_id | category_id
INSERT IGNORE INTO plugin_sid (plugin_id, sid, reliability,
                        priority, subcategory_id,
                        category_id, name) VALUES (@pluginid, 1, 1, 1, 11, 19, 'elastichoney: Attack Detected');
INSERT IGNORE INTO plugin_sid (plugin_id, sid, reliability,
                        priority, subcategory_id,
                        category_id, name) VALUES (@pluginid, 2, 1, 1, 11, 19, 'elastichoney: Recon Detected');
```

Oluşturulan SQL Dosyası OSSIM DB import idilir

```
ossim-db < /usr/share/doc/ossim-mysql/contrib/plugins/elastichoney.sql
```

3- Hem OSSIM üzerinde hemde gönderici üzerinde Syslog yapılandırmasını yapılır.

A- /etc/rsyslog.d/elastichoney.conf

```
#AlienVault OSSIM Server Rsyslog
#Conf Start
if $fromhost-ip == '169.254.2.254' and $programname == "elastichoney" then /var/log/elastichoney.log
& ~
#End of Conf
```

B - Client(Honeypoy) Rsyslog /etc/rsyslog.d/elastichoney.conf

```
#Only needs to be loaded once, like most rsyslog modules
$ModLoad imfile

#path to the file which you want to monitor
$InputFileName /var/log/elastichoney/elastichoney.log

#The tag apache can be changed to whatever you'd like
$InputFileTag elastichoney:

#the name of file within rsyslogs working directory
$InputFileStateFile elastichoney-stat

#By default this is set to 'notice'
$InputFileSeverity notice

#This is necessary for file monitoring (no parameters)
$InputRunFileMonitor

#Set to how often the file should be polled. (default = 10s)
$InputFilePollInterval 1

# This is a template for Loggly. Substitute your Customer Token for TOKEN
#$template LogglyFormatAccess,"%protocol-version% %HOSTNAME% %app-name% %msg%\n"
$template LogglyFormat,"%HOSTNAME% %app-name% %msg%\n"
#$template LogglyFormatAccess,"<%pri%>%protocol-version% %timestamp:::date-rfc3339% %HOSTNAME% %app-name%
%procid% %msgid% [TOKEN@41058 tag=\"Access\"] %msg%\n"
#$template LogglyFormatAccess,"<%pri%>%protocol-version% %timestamp:::date-rfc3339% %HOSTNAME% %app-name%
%procid% %msgid% [TOKEN@41058 tag=\"apache\"] %msg%\n"
# Make sure the template above is on one line.

if $programname == 'elastichoney' then @169.254.1.150:514;LogglyFormat
```

4- OSSIM Logrotate ayar dosyası oluşturulur.

```
/var/log/elastichoney.log {
        weekly
        missingok
        rotate 7
        compress
        notifempty
}
```

5- Rsyslog servisi her iki cihazda da yeniden başlatılır.

```
systemctl restart rsyslog
```

6- "alienvault-setup" komutu ile Sensör ayarlarından plugin aktif edilir.

```
alienvault-setup > configure sensor > configure data source plugins > [x] elastichoney
```

veya

Aşağıdaki config.cfg dosyasında plugins section'a ilgili satır eklenir.

Ayar Dosyası: /etc/ossim/agent/config.cfg

Eklenecek satır: elastichoney=/etc/ossim/agent/plugins/elastichoney.cfg

```
sed -i "/^\[plugins/,/^$/ s|^$|elastichoney=/etc/ossim/agent/plugins/elastichoney.cfg\n|" /etc/ossim/agent/config.cfg
```

ve

Aşağıdaki ossim_setup.conf ayar dosyasındaki [sensor] bölümündeki detectors değişkenine eklenmelidir.

/etc/ossim/ossim_setup.conf

```
....

[sensor]
asec=no
detectors=ssh, shockpot, sudo, ssh-pardus, ossec-single-line, pam_unix, prads, suricata, elastichoney

....
```

7- Seçim yapıldıktan sonra geri ana ekrana dönülür ve seçim uygulanır.

```
alienvault-setup > Apply all changes
```

veya

```
alienvault-reconfig --quiet veya --console-log
```

8- OSSIM web arabirimiden kayıtlar izlenir.

```
https://ossim_ip_address > Analysis > Security Events > Real Time
```

Yardımcı SQL Sorguları

```
#Mysql
export myhost=$(grep "^db_ip" /etc/ossim/ossim_setup.conf|cut -d"=" -f 2)
export myuser=$(grep "^user" /etc/ossim/ossim_setup.conf|cut -d"=" -f 2)
export mypass=$(grep "^pass" /etc/ossim/ossim_setup.conf|cut -d"=" -f 2)
plugin_id=91111

#Plugin
mysql -h ${myhost} -u ${myuser} -p${mypass} alienvault -e "select * from plugin where id = '${plugin_id}' "

#plugin sid control
mysql -h ${myhost} -u ${myuser} -p${mypass} alienvault -e "select * from plugin_sid where plugin_id = '${plugin_id}' "

#Product Type List
mysql -h ${myhost} -u ${myuser} -p${mypass} alienvault -e "select * from product_type"

#category List
mysql -h ${myhost} -u ${myuser} -p${mypass} alienvault -e "select * from category"

#Sub Category List
mysql -h ${myhost} -u ${myuser} -p${mypass} alienvault -e "select * from subcategory"
```