入侵偵測系統結合大數據分析:
Suricata 與 ELK Stack 之實際應用

中山大學(高屏澎區網中心)

王聖全

Agenda

- Suricata 簡介及安裝
- ELK stack與Suricata整合之應用
- Suricata偵測規則運作及探討
- Suricata實例應用

Suricata 簡介及安裝

Suricata Introduction

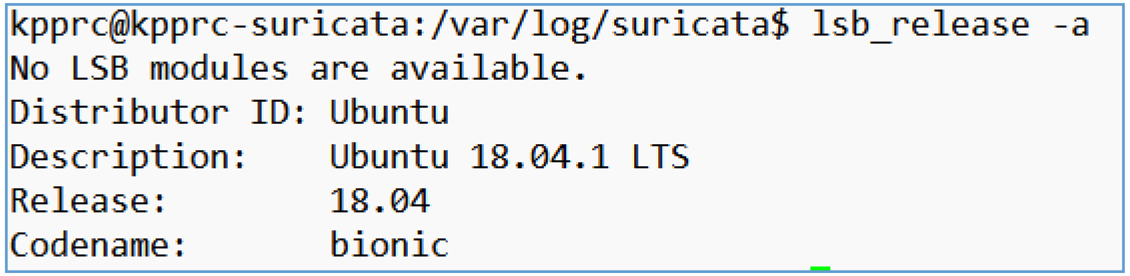
- Network Intrusion Detection System (NIDS) engine
- Network Intrusion Prevention System (NIPS) engine
- Network Security Monitoring (NSM) engine
- Off line analysis of PCAP files
- Traffic recording using pcap logger
- Unix socket mode for automated PCAP file processing
- Advanced integration with Linux Netfilter firewalling
- Open Source: GPLv2 License

NSM

- Network Security Monitoring
- Generate “alerts”
- Information events like HTTP, TLS, SSH
- Full Packet Capture
    - Incident analysis

Environment Setup

- Running OS
  - Ubuntu 18.04.1 LTS (64bit version)



```
kpprc@kpprc-suricata:/var/log/suricata$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.1 LTS
Release:        18.04
Codename:       bionic
```

- Suricata Stable Version
  - Newest version now: 4.0.5

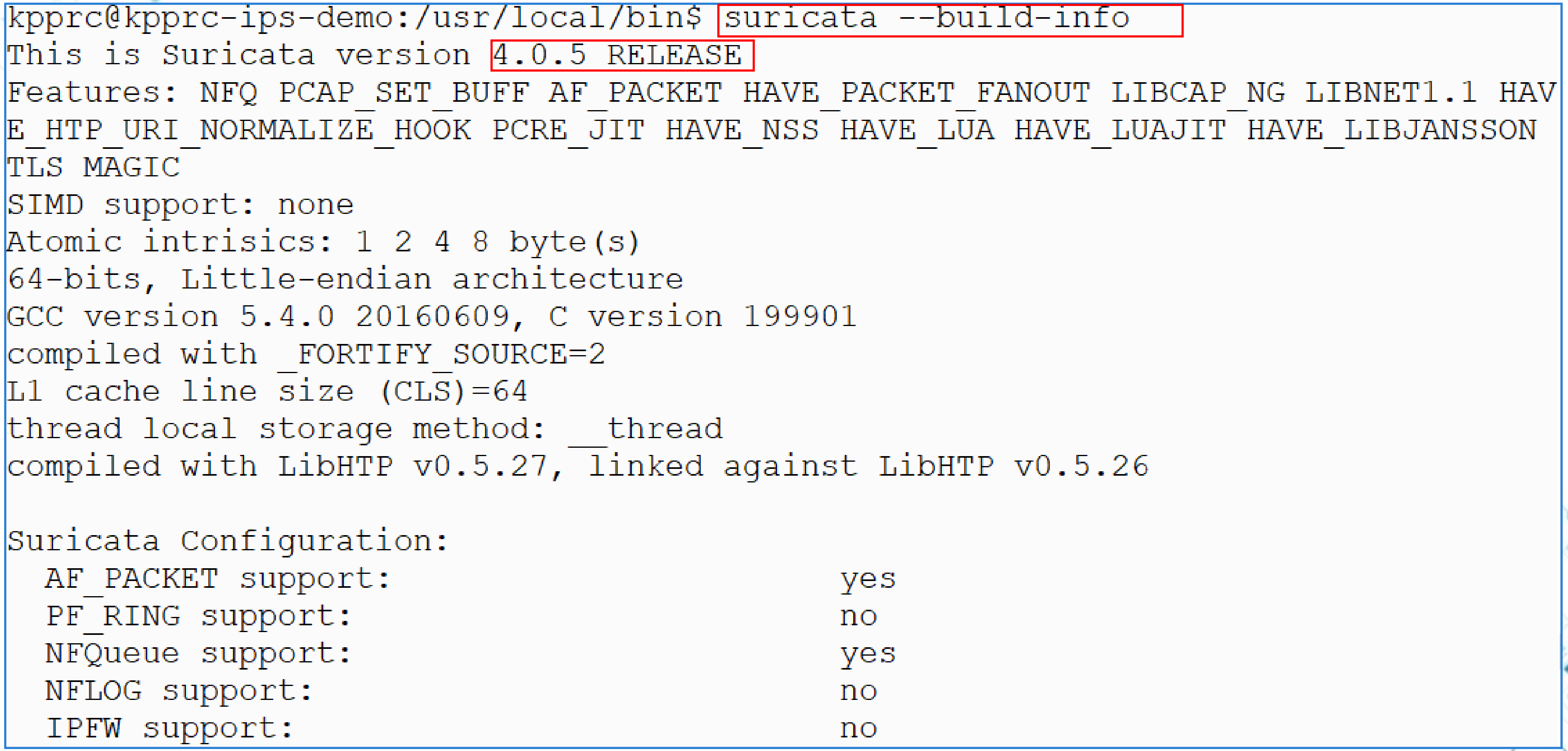
Ubuntu install dependencies

- sudo apt-get install libpcre3 libpcre3-dbg libpcre3-dev build-essential libpcap-dev libnet1-dev libyaml-0-2 libyaml-dev pkg-config zlib1g zlib1g-dev libcap-ng-dev libcap-ng0 make libmagic-dev libjansson-dev libnss3-dev libgeoip-dev liblua5.1-dev libhiredis-dev libevent-dev

Suricata Installation

- sudo add-apt-repository ppa:oisf/suricata-stable
- sudo apt-get update
- sudo apt-get install suricata

Suricata Version Check



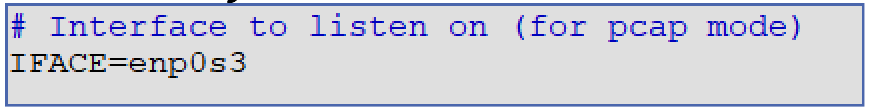
```
kpprc@kpprc-ips-demo:/usr/local/bin$ suricata --build-info
This is Suricata version 4.0.5 RELEASE
Features: NFQ PCAP_SET_BUFF AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HAV
E_HTP_URI_NORMALIZE_HOOK PCRE_JIT HAVE_NSS HAVE_LUA HAVE_LUAJIT HAVE_LIBJANSSON
TLS MAGIC
SIMD support: none
Atomic intrisics: 1 2 4 8 byte(s)
64-bits, Little-endian architecture
GCC version 5.4.0 20160609, C version 199901
compiled with _FORTIFY_SOURCE=2
L1 cache line size (CLS)=64
thread local storage method: __thread
compiled with LibHTP v0.5.27, linked against LibHTP v0.5.26

Suricata Configuration:
  AF_PACKET support:                       yes
  PF_RING support:                         no
  NFQueue support:                         yes
  NFLOG support:                           no
  IPFW support:                            no
```

Suricata configuration setting overview

1. Inform Suricata about your network
2. Select the rules to enable or disable
3. Select outputs to enable
4. Configure common capture settings
5. App Layer Protocol Configuration

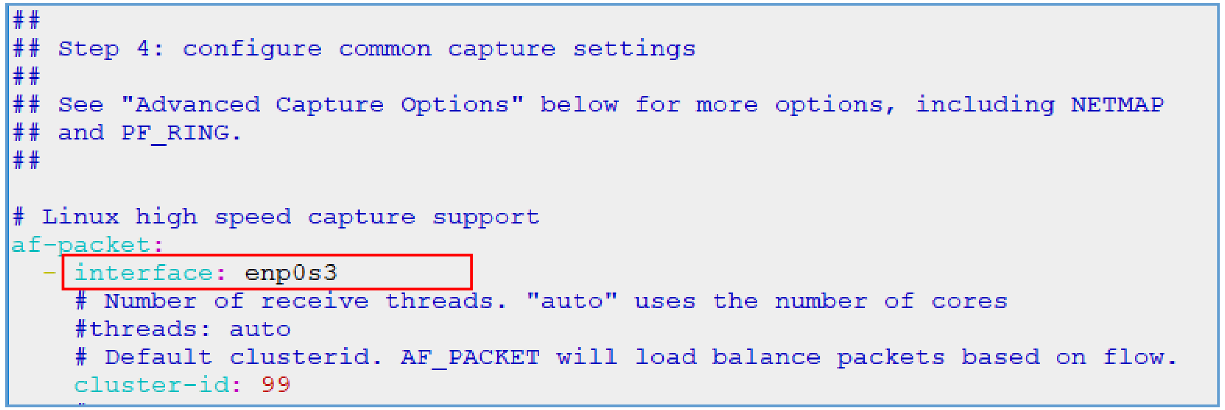
Interface and Default file configuration

- Set interface to promiscuous mode
  - ifconfig <*IFACE*> promisc
- /etc/default/suricata
  - change <*IFACE*> parameter
    - eth0 to < *your network interface name*> (**enp0s3**)



```
# Interface to listen on (for pcap mode)
IFACE=enp0s3
```

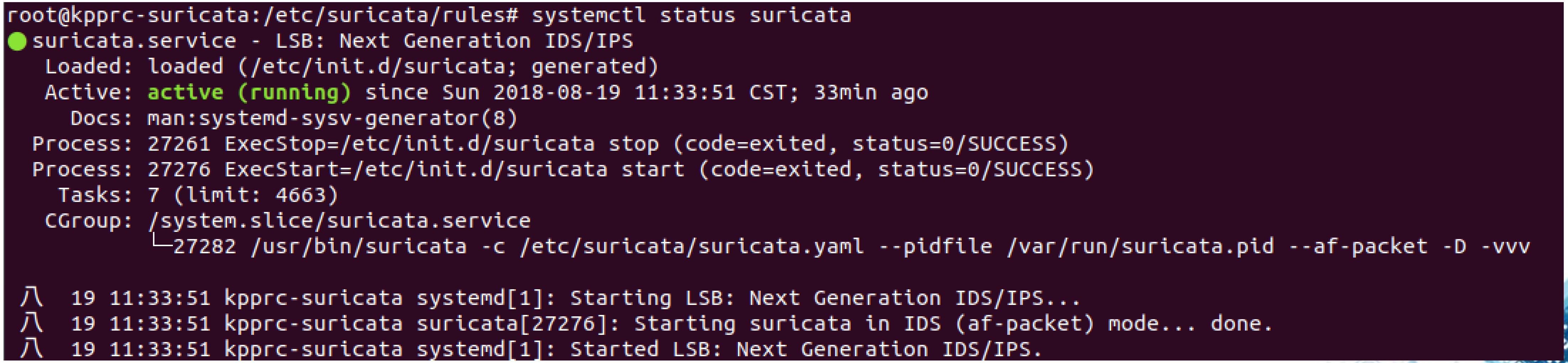
- /etc/suricata/suricata.yml
  - Change interface parameter below (default are all eth0)
    - af-packet
    - pcap
    - pfring
    - netmap



```
##
## Step 4: configure common capture settings
##
## See "Advanced Capture Options" below for more options, including NETMAP
## and PF_RING.
##

# Linux high speed capture support
af-packet:
  - interface: enp0s3
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
```

Let’s start

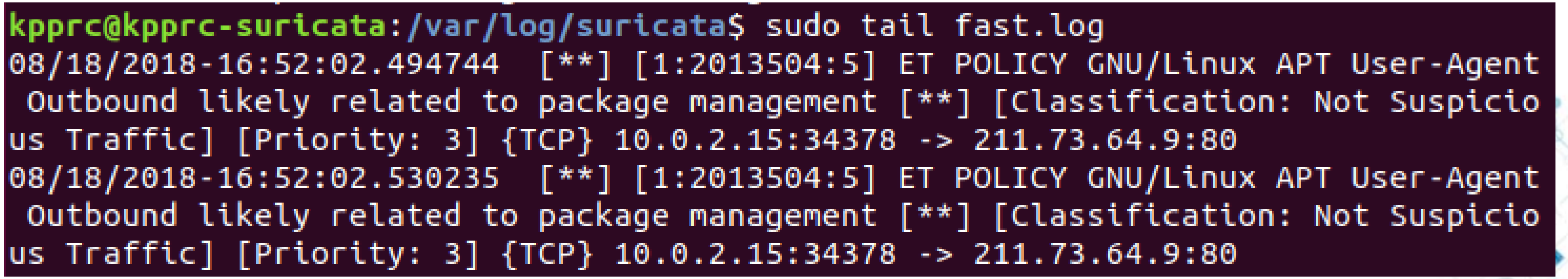
- Running Suricata
  - sudo /etc/init.d/suricata start
- Running Status



```
root@kpprc-suricata:/etc/suricata/rules# systemctl status suricata
● suricata.service - LSB: Next Generation IDS/IPS
   Loaded: loaded (/etc/init.d/suricata; generated)
   Active: active (running) since Sun 2018-08-19 11:33:51 CST; 33min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 27261 ExecStop=/etc/init.d/suricata stop (code=exited, status=0/SUCCESS)
  Process: 27276 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)
    Tasks: 7 (limit: 4663)
   CGroup: /system.slice/suricata.service
           └─27282 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid --af-packet -D -vvv

 八  19 11:33:51 kpprc-suricata systemd[1]: Starting LSB: Next Generation IDS/IPS...
 八  19 11:33:51 kpprc-suricata suricata[27276]: Starting suricata in IDS (af-packet) mode... done.
 八  19 11:33:51 kpprc-suricata systemd[1]: Started LSB: Next Generation IDS/IPS.
```

Suricata Output Files (1/2)

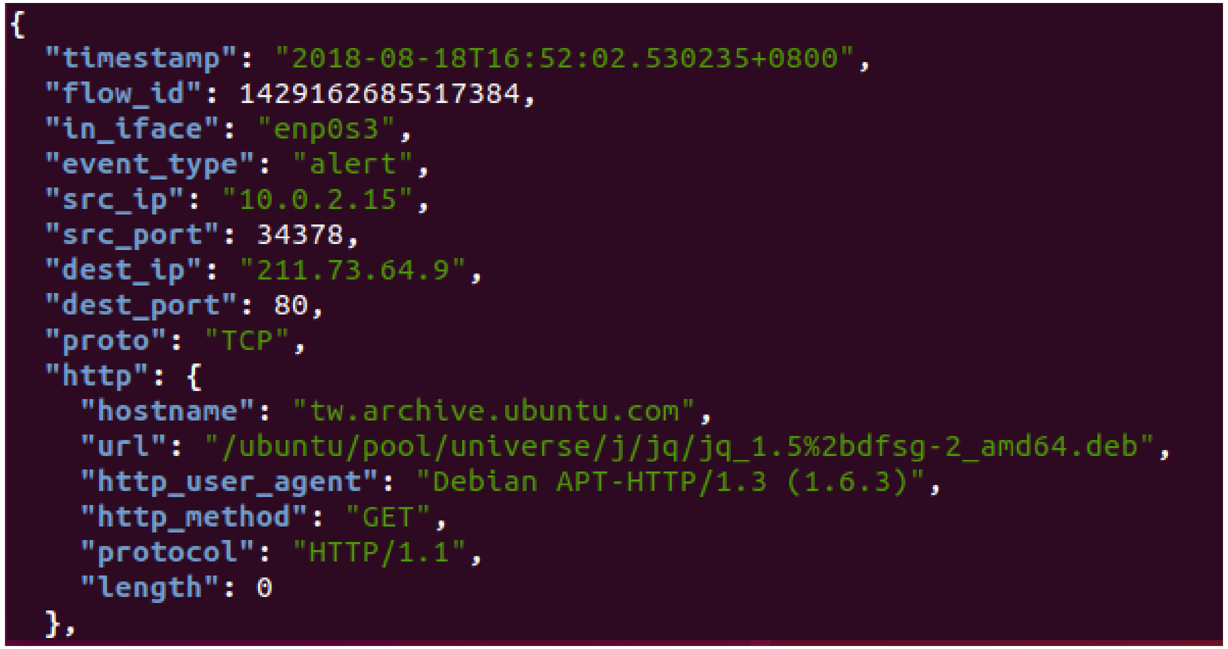
- Default PATH
  - /var/log/suricata
- fast.log
  - Line based alerts log
  - Alerts consisting of a single line



```
kpprc@kpprc-suricata:/var/log/suricata$ sudo tail fast.log
08/18/2018-16:52:02.494744  [**] [1:2013504:5] ET POLICY GNU/Linux APT User-Agent
 Outbound likely related to package management [**] [Classification: Not Suspicio
us Traffic] [Priority: 3] {TCP} 10.0.2.15:34378 -> 211.73.64.9:80
08/18/2018-16:52:02.530235  [**] [1:2013504:5] ET POLICY GNU/Linux APT User-Agent
 Outbound likely related to package management [**] [Classification: Not Suspicio
us Traffic] [Priority: 3] {TCP} 10.0.2.15:34378 -> 211.73.64.9:80
```

Suricata Output Files (2/2)

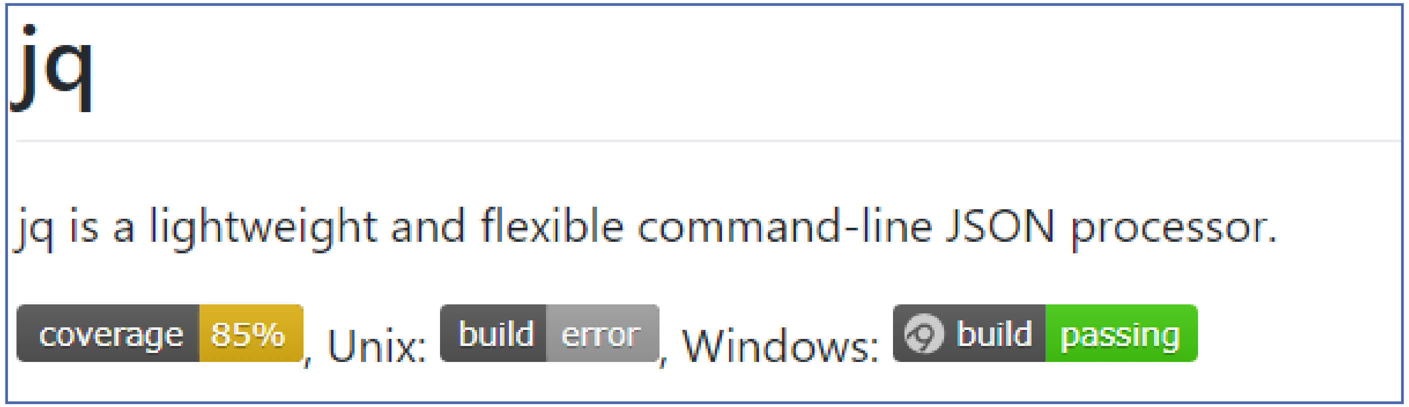
- Suricata Eve **(Extensible Event Format)** JSON Output
- Filename: eve.json
- JSON output for alerts and events



```
{
  "timestamp": "2018-08-18T16:52:02.530235+0800",
  "flow_id": 1429162685517384,
  "in_iface": "enp0s3",
  "event_type": "alert",
  "src_ip": "10.0.2.15",
  "src_port": 34378,
  "dest_ip": "211.73.64.9",
  "dest_port": 80,
  "proto": "TCP",
  "http": {
    "hostname": "tw.archive.ubuntu.com",
    "url": "/ubuntu/pool/universe/j/jq/jq_1.5%2bdfsg-2_amd64.deb",
    "http_user_agent": "Debian APT-HTTP/1.3 (1.6.3)",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "length": 0
  },
```

Looking at EVE.json

- Use standard UNIX tool
  - Grep, awk, sed (not so efficient)
- Recommended Tool
  - **jq**: tool dedicated to the transformation/parsing of a JSON entry
- Installation
  - sudo apt-get install jq



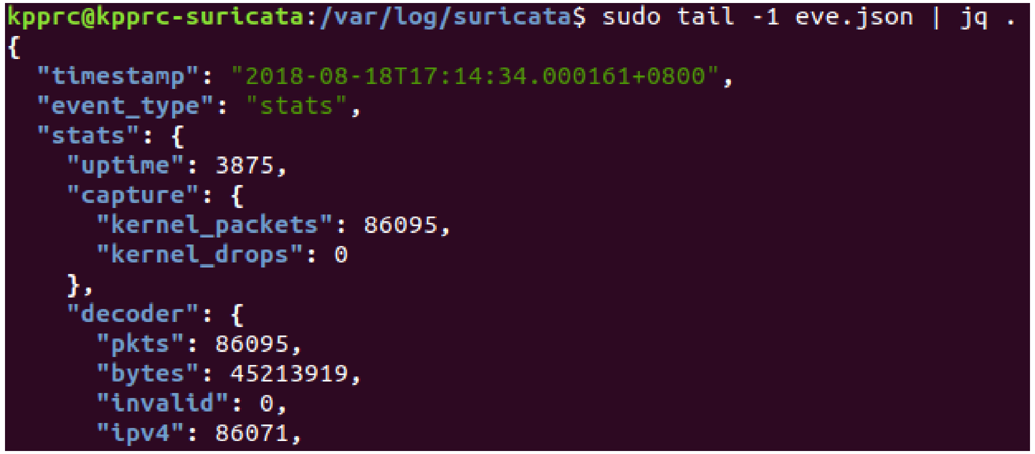
jq

jq is a lightweight and flexible command-line JSON processor.

coverage 85%, Unix: build error, Windows: build passing

Lab1

- Beautify EVE.json format using jq utility
  - tail -n 1 eve.json | jq '.’
  - tail -n 1 eve.json | jq -c '.‘
  - cat eve.json | jq 'select (.event_type == "http")’
  - cat eve.json | jq 'select (.event_type == "ssh") | .ssh.client'
  - jq .src_ip eve.json



```
kpprc@kpprc-suricata:/var/log/suricata$ sudo tail -1 eve.json | jq .
{
  "timestamp": "2018-08-18T17:14:34.000161+0800",
  "event_type": "stats",
  "stats": {
    "uptime": 3875,
    "capture": {
      "kernel_packets": 86095,
      "kernel_drops": 0
    },
    "decoder": {
      "pkts": 86095,
      "bytes": 45213919,
      "invalid": 0,
      "ipv4": 86071,
```

Eve JSON Format (1/3)

```
{
    "timestamp": "2009-11-24T21:27:09.534255",
    "event_type": "alert",
    "src_ip": "192.168.2.7",
    "src_port": 1041,
    "dest_ip": "x.x.250.50",
    "dest_port": 80,
    "proto": "TCP",
    "alert": {
        "action": "allowed",
        "gid": 1,
        "signature_id" :2001999,
        "rev": 9,
        "signature": "ET MALWARE BTGrab.com Spyware Downloading Ads",
        "category": "A Network Trojan was detected",
        "severity": 1
    }
}
```

Eve JSON Format (2/3)

- Common Section

```
{"timestamp":"2009-11-24T21:27:09.534255","event_type":"TYPE", ...tuple... ,"TYPE":{ ... type specific content ... }}
```

- Event types
  - indicate the log type
    - Alert
    - HTTP
    - DNS
    - TLS

Eve JSON Format (3/3)

- Event type: DNS

```
"dns": {
    "type": "query",
    "id": 16000,
    "rrname": "twitter.com",
    "rrtype":"A"
}
```

```
"dns": {
    "type": "answer",
    "id":16000,
    "rrname": "twitter.com",
    "rrtype":"A",
    "ttl":8,
    "rdata": "199.16.156.6"
}
```

“rrname”: Resource Record Name (e.g.: a domain name)
“rrtype”: Resource Record Type (e.g.: A, AAAA, NS, PTR)

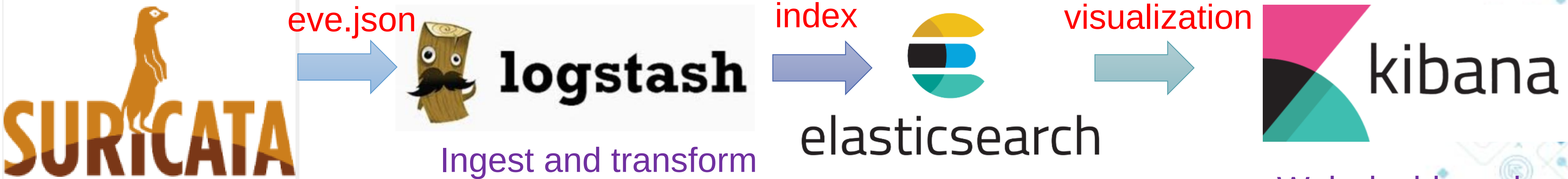
Alert Log Case Study

```
{
  "timestamp": "2018-08-17T06:17:55.254631+0800",
  "flow_id": 1882149025350136,
  "in_iface": "ens2f1",
  "event_type": "alert",
  "vlan": 101,
  "src_ip": "123.207.243.X",
  "src_port": 59821,
  "dest_ip": "163.28.X.X",
  "dest_port": 445,
  "proto": "TCP",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2024297,
    "rev": 2,
    "signature": "ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010",
    "category": "Attempted Administrator Privilege Gain",
    "severity": 1
  }, …
}
```

ELK Stack與Suricata 整合之應用

Suricata with ELK Stack Integration

- Suricata: 4.0.5 stable version
- Logstash: data pipeline
- Elasticsearch: database
- Kibana: Visualization and dashboards



eve.json

index

visualization

Alert messages

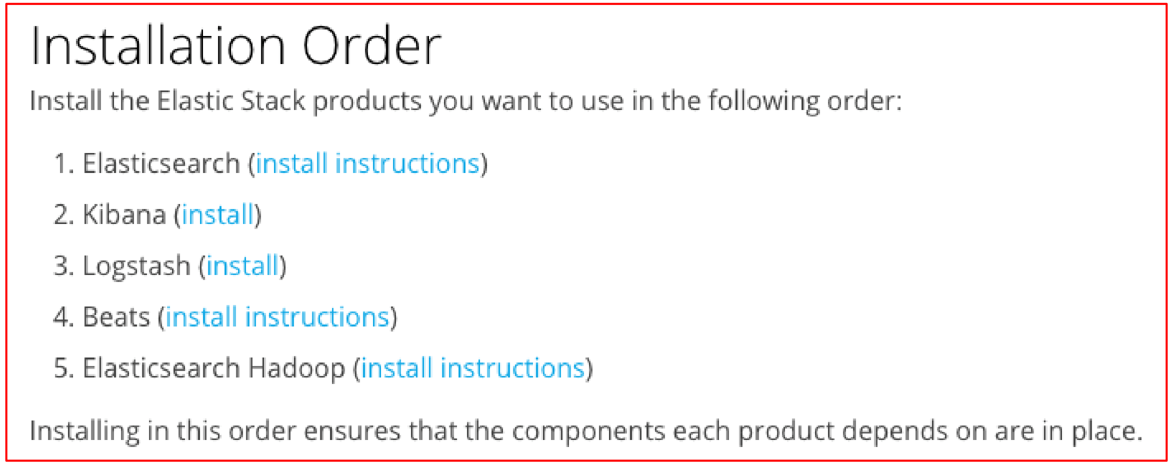
Ingest and transform messages

search

Web dashborads

ELK Stack

- **Use the same version across the entire stack**.
  - E.g., Elasticsearch 6.3.0, Kibana 6.3.0, and Logstash 6.3.0.

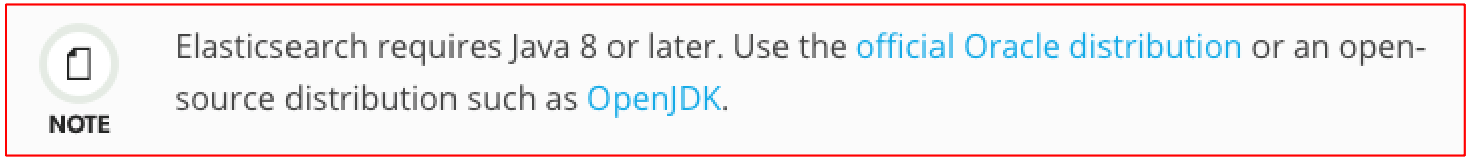


Installation Order

Install the Elastic Stack products you want to use in the following order:

1. Elasticsearch (install instructions)
2. Kibana (install)
3. Logstash (install)
4. Beats (install instructions)
5. Elasticsearch Hadoop (install instructions)

Installing in this order ensures that the components each product depends on are in place.



NOTE

Elasticsearch requires Java 8 or later. Use the official Oracle distribution or an open-source distribution such as OpenJDK.

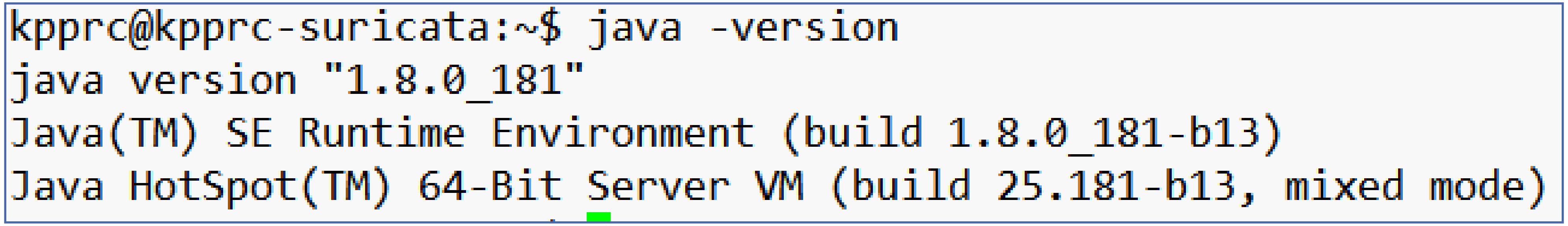
https://www.elastic.co/guide/en/elastic-stack/current/installing-elastic-stack.html#installing-elastic-stack

Install JAVA

- $ sudo apt-get install software-properties-common
- $ sudo add-apt-repository ppa:webupd8team/java
- $ sudo apt-get update
- $ sudo apt-get install oracle-java8-installer
- 在/etc/profile檔案加上環境變數
  - export JAVA_HOME=/usr/lib/jvm/java-8-oracle
  - export JRE_HOME=/usr/lib/jvm/java-8-oracle/jre
- $ sudo apt-get install oracle-java8-set-default

Install JAVA (cont.)

- $ java -version (確認安裝結果)



```
kpprc@kpprc-suricata:~$ java -version
java version "1.8.0_181"
Java(TM) SE Runtime Environment (build 1.8.0_181-b13)
Java HotSpot(TM) 64-Bit Server VM (build 25.181-b13, mixed mode)
```

Elasticsearch Installation

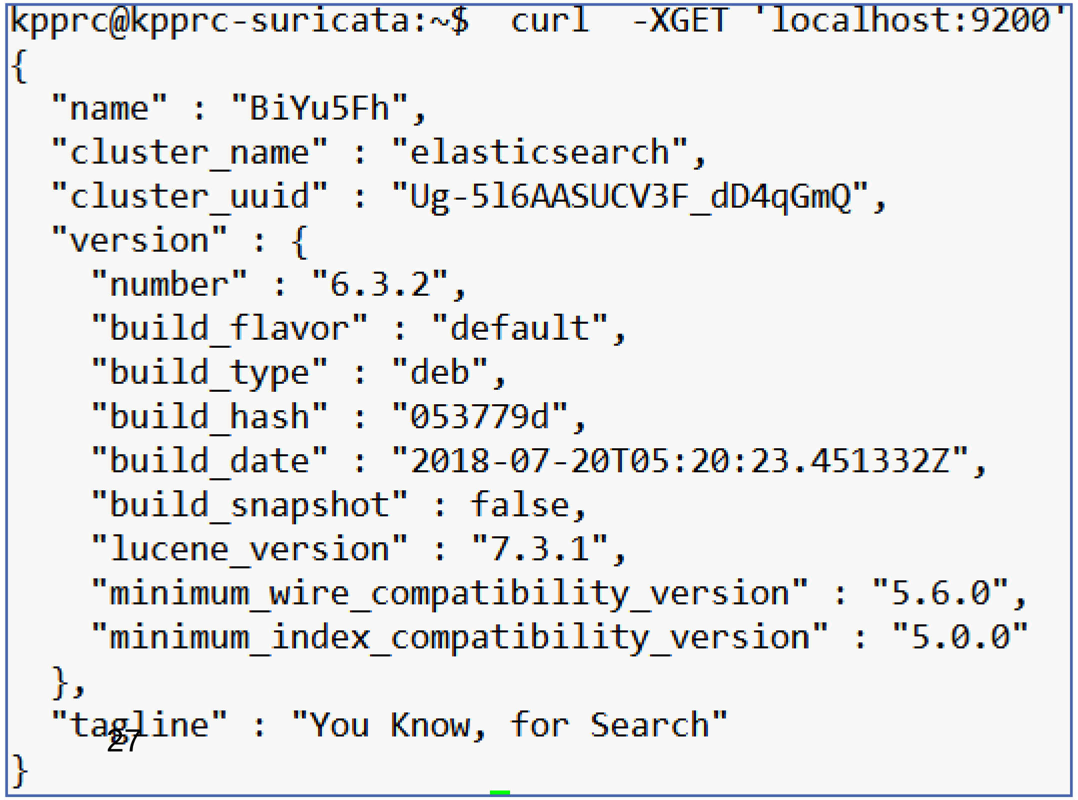
- wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
- sudo apt-get install apt-transport-https
- echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-6.x.list
- sudo apt-get update && sudo apt-get install elasticsearch
- sudo /bin/systemctl daemon-reload
- sudo /bin/systemctl enable elasticsearch.service
- sudo systemctl start elasticsearch.service

https://www.elastic.co/guide/en/elasticsearch/reference/6.3/deb.html

Check Elasticsearch Status

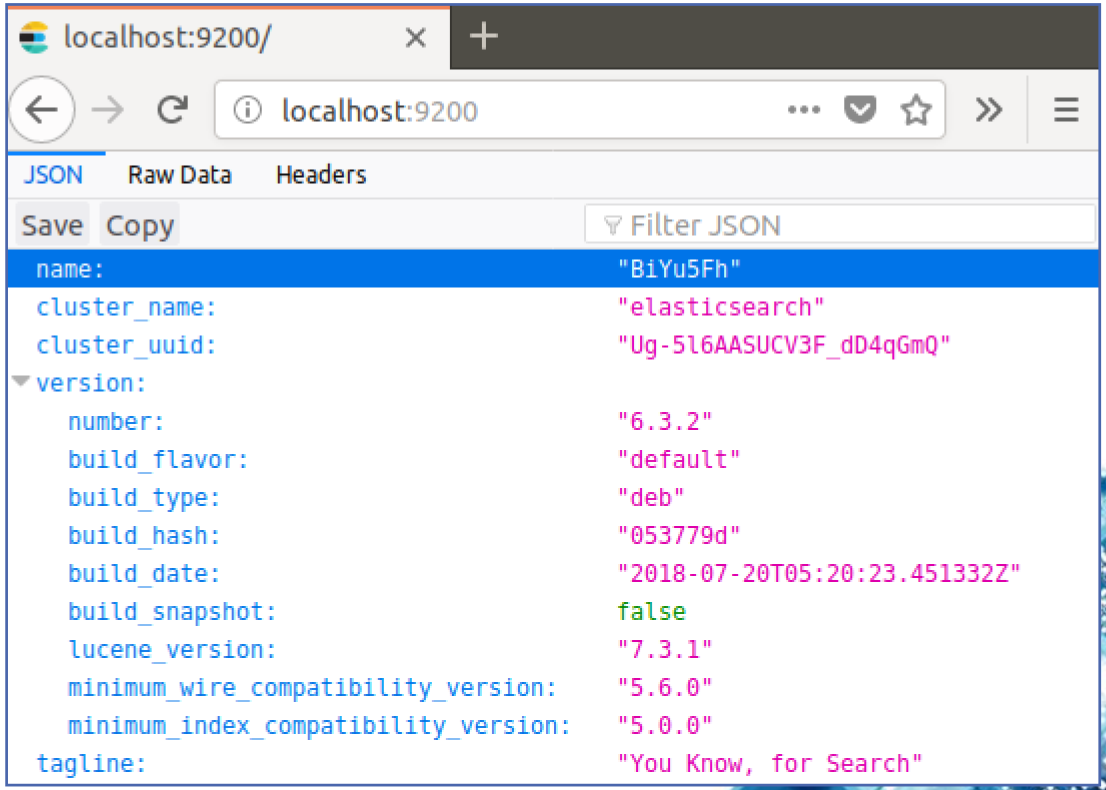
- Check Elasticsearch version and status
  - sudo apt-get install curl

Command line



```
kpprc@kpprc-suricata:~$  curl  -XGET 'localhost:9200'
{
  "name" : "BiYu5Fh",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "Ug-5l6AASUCV3F_dD4qGmQ",
  "version" : {
    "number" : "6.3.2",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "053779d",
    "build_date" : "2018-07-20T05:20:23.451332Z",
    "build_snapshot" : false,
    "lucene_version" : "7.3.1",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Web

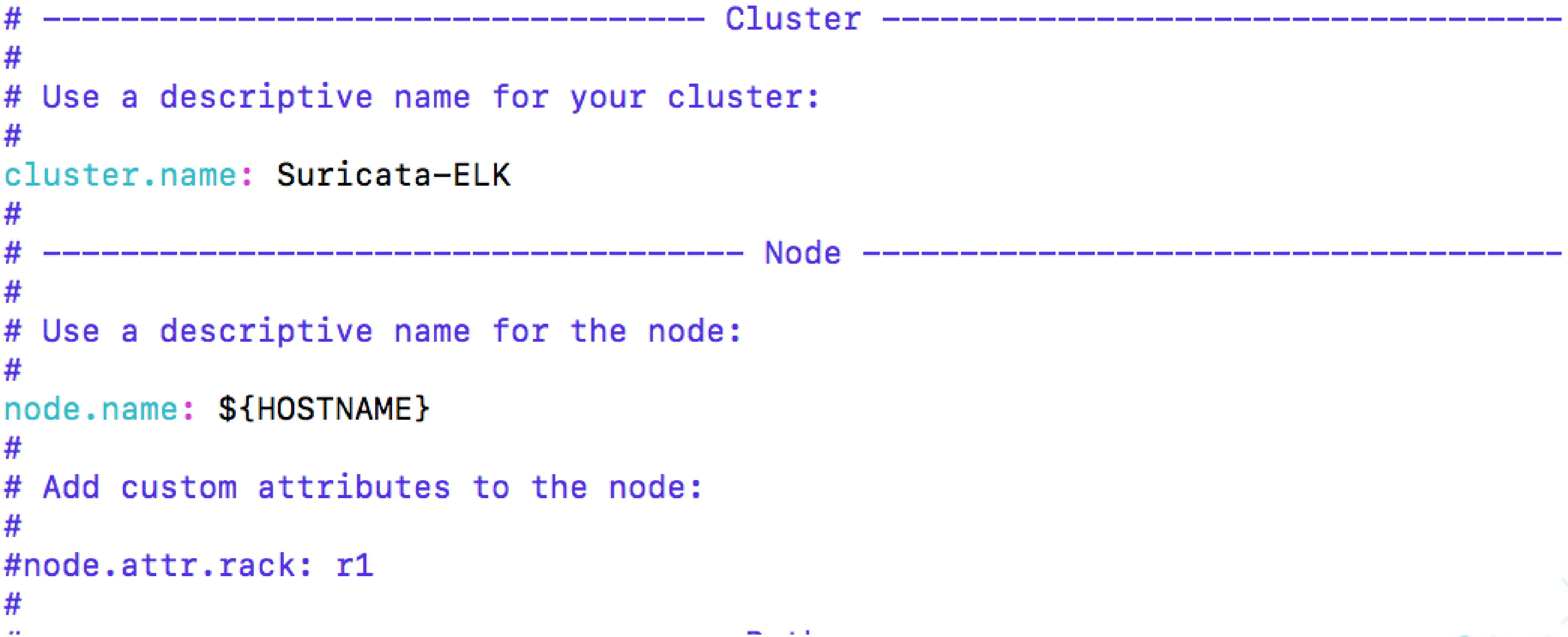


```
name:                                   "BiYu5Fh"
cluster_name:                           "elasticsearch"
cluster_uuid:                           "Ug-5l6AASUCV3F_dD4qGmQ"
▼version:
  number:                               "6.3.2"
  build_flavor:                         "default"
  build_type:                           "deb"
  build_hash:                           "053779d"
  build_date:                           "2018-07-20T05:20:23.451332Z"
  build_snapshot:                       false
  lucene_version:                       "7.3.1"
  minimum_wire_compatibility_version:   "5.6.0"
  minimum_index_compatibility_version:  "5.0.0"
tagline:                                "You Know, for Search"
```

Configuring Elasticsearch

- elasticsearch.yml
  - configuring Elasticsearch
- jvm.options
  - configuring Elasticsearch JVM settings
- log4j2.properties
  - configuring Elasticsearch logging

Configuring Elasticsearch(cont.)

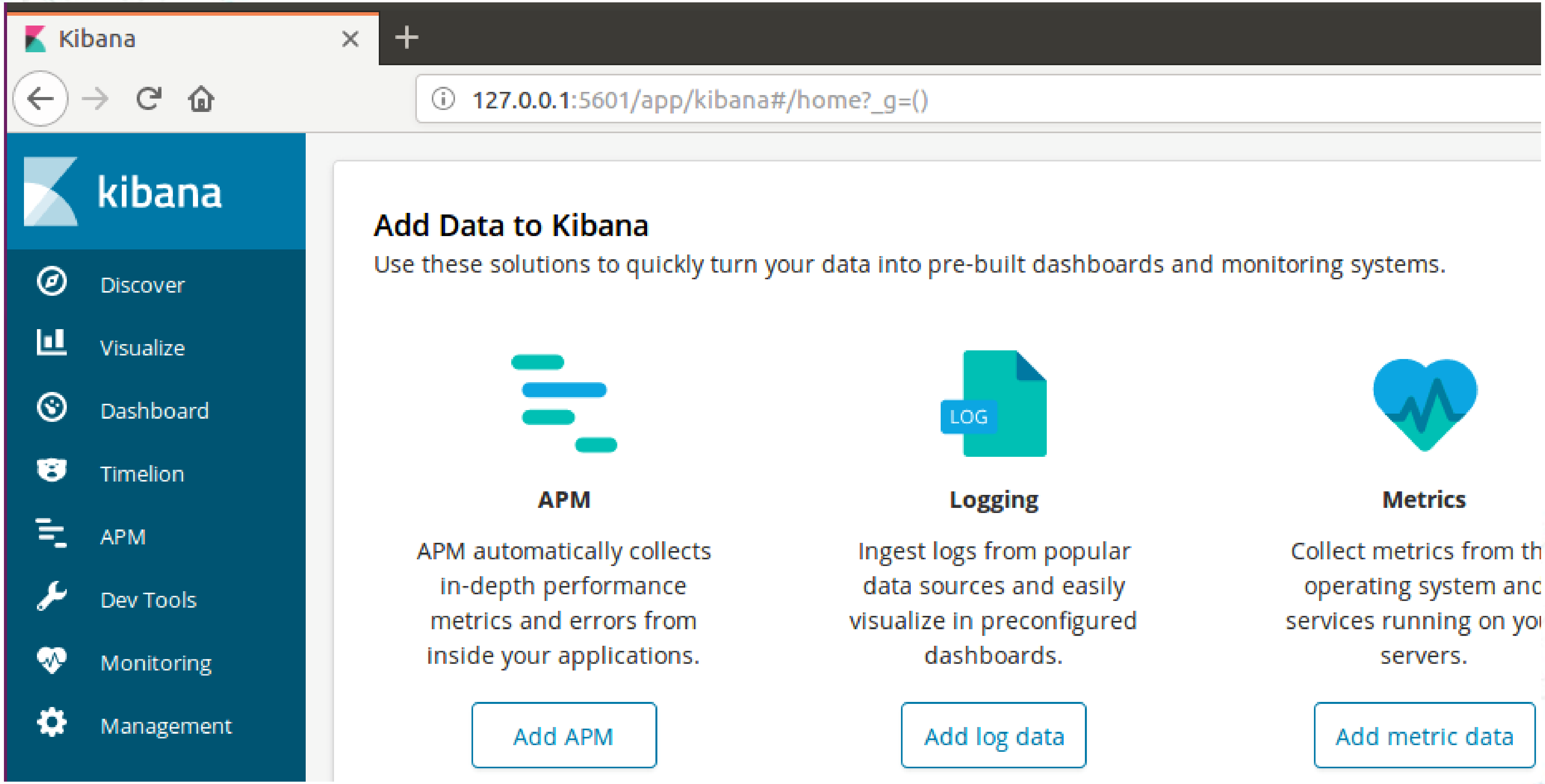


```
# ---------------------------------- Cluster -----------------------------------
#
# Use a descriptive name for your cluster:
#
cluster.name: Suricata-ELK
#
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
node.name: ${HOSTNAME}
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
#
```

Kibana Installation

- sudo apt-get update && sudo apt-get install kibana
- sudo /bin/systemctl daemon-reload
- sudo /bin/systemctl enable kibana.service
- sudo systemctl start kibana.service

Check Kibana Status



Add Data to Kibana

Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Add APM

Logging

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Add log data

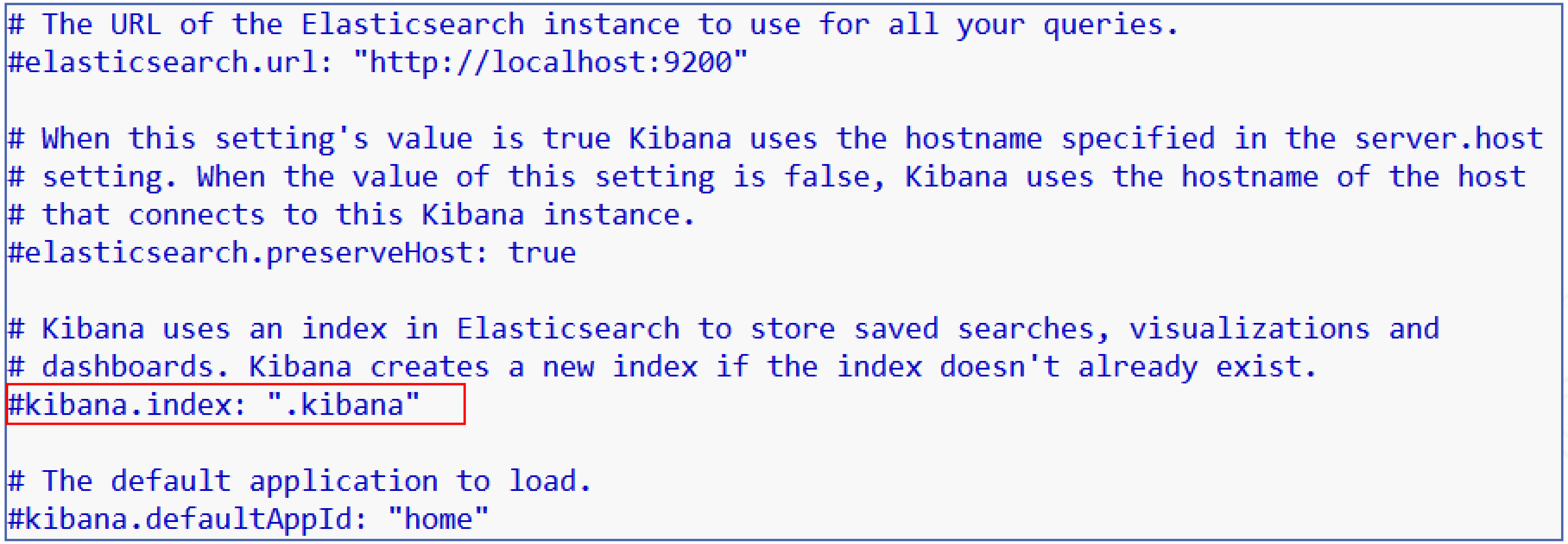
Metrics

Collect metrics from th operating system anc services running on yo servers.

Add metric data

Configuring Kibana

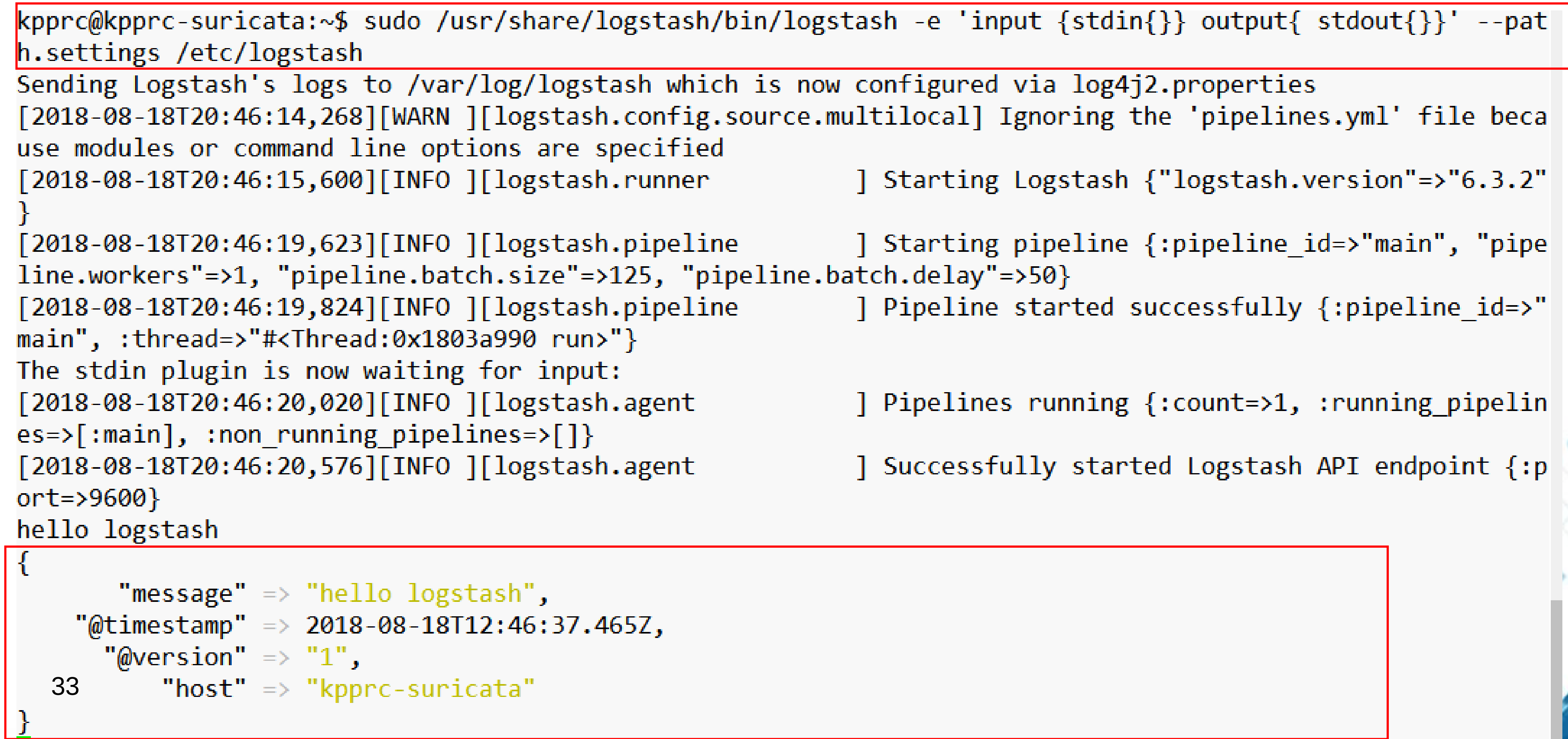
- Config file: /etc/kibana/kibana.yaml
- Default run on
    - http://127.0.0.1:5601



```
# The URL of the Elasticsearch instance to use for all your queries.
#elasticsearch.url: "http://localhost:9200"

# When this setting's value is true Kibana uses the hostname specified in the server.host
# setting. When the value of this setting is false, Kibana uses the hostname of the host
# that connects to this Kibana instance.
#elasticsearch.preserveHost: true

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
#kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"
```

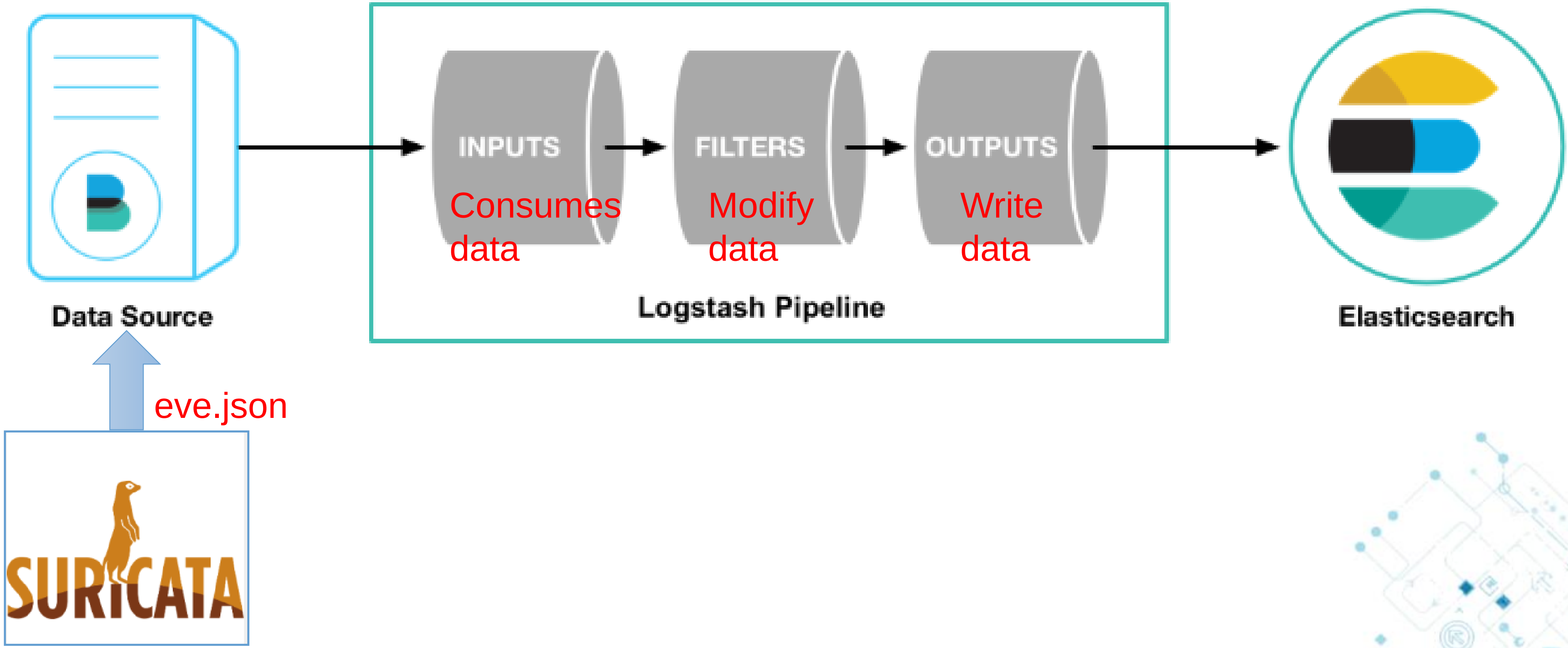
Logstash Installation

- sudo apt-get update && sudo apt-get install logstash
- sudo /usr/share/logstash/bin/logstash -e 'input {stdin{}} output{ stdout{}}' --path.settings /etc/logstash



```
kpprc@kpprc-suricata:~$ sudo /usr/share/logstash/bin/logstash -e 'input {stdin{}} output{ stdout{}}' --pat
h.settings /etc/logstash
Sending Logstash's logs to /var/log/logstash which is now configured via log4j2.properties
[2018-08-18T20:46:14,268][WARN ][logstash.config.source.multilocal] Ignoring the 'pipelines.yml' file beca
use modules or command line options are specified
[2018-08-18T20:46:15,600][INFO ][logstash.runner          ] Starting Logstash {"logstash.version"=>"6.3.2"
}
[2018-08-18T20:46:19,623][INFO ][logstash.pipeline        ] Starting pipeline {:pipeline_id=>"main", "pipe
line.workers"=>1, "pipeline.batch.size"=>125, "pipeline.batch.delay"=>50}
[2018-08-18T20:46:19,824][INFO ][logstash.pipeline        ] Pipeline started successfully {:pipeline_id=>"
main", :thread=>"#<Thread:0x1803a990 run>"}
The stdin plugin is now waiting for input:
[2018-08-18T20:46:20,020][INFO ][logstash.agent           ] Pipelines running {:count=>1, :running_pipelin
es=>[:main], :non_running_pipelines=>[]}
[2018-08-18T20:46:20,576][INFO ][logstash.agent           ] Successfully started Logstash API endpoint {:p
ort=>9600}
hello logstash
{
       "message" => "hello logstash",
    "@timestamp" => 2018-08-18T12:46:37.465Z,
      "@version" => "1",
          "host" => "kpprc-suricata"
}
```

Logstash integration with Suricata



Logstash configuration(1/3)

```
input {
  file {
  path => ["/var/log/suricata/eve.json"]
  sincedb_path => ["/var/lib/logstash/since.db"]
  codec => json
  type => "SuricataIDPS"
 }
}
```

Logstash configuration(2/3)

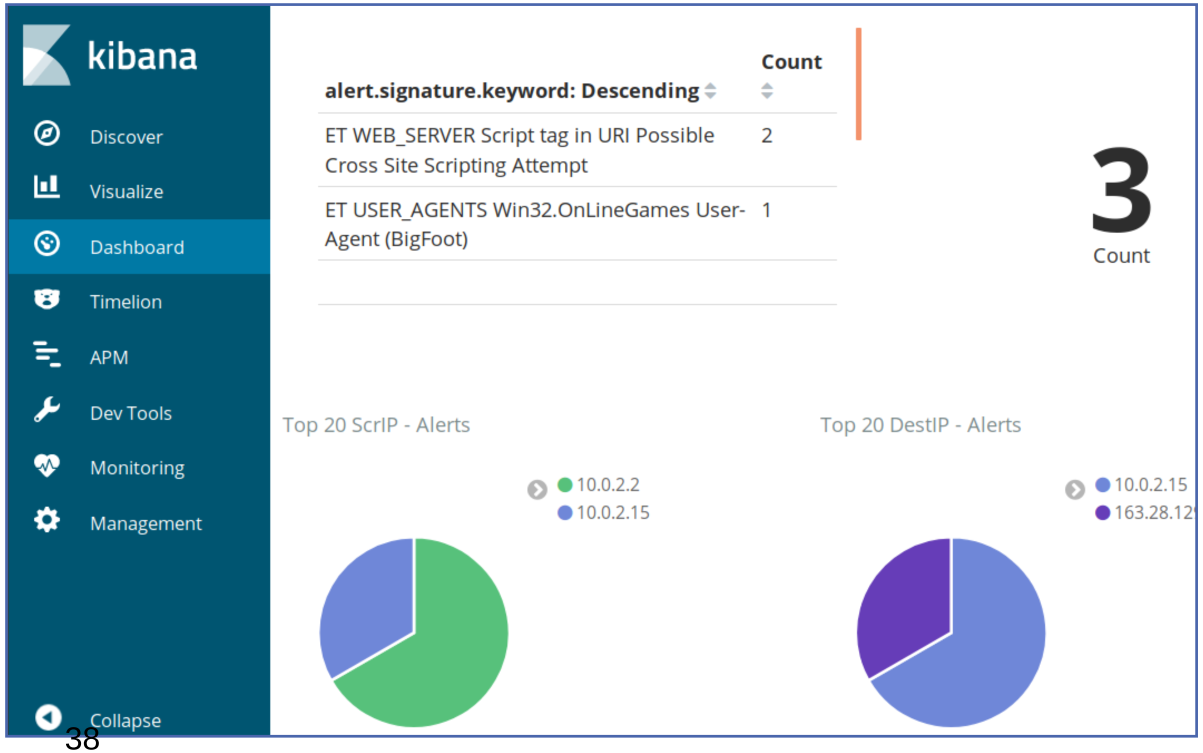
```
filter {
      if [type] == "SuricataIDPS" {
      date {
      match => [ "timestamp", "ISO8601" ]
      }
      ruby {
      code => "
      if event.get('[event_type]') == 'fileinfo'
      event.set('[fileinfo][type]',
     event.get('[fileinfo][magic]').to_s.split(',')[0])
      end
      "

 }
```

Logstash configuration(3/3)

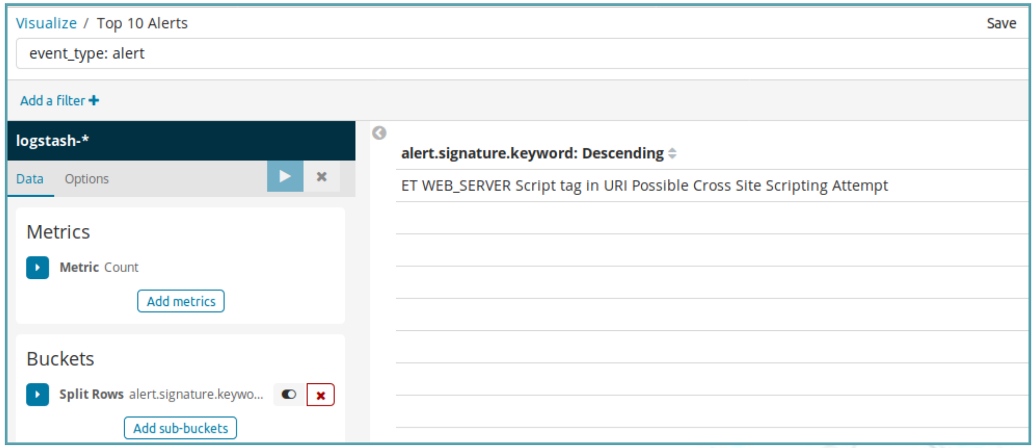
```
output {
    elasticsearch {
    hosts => localhost
    index => "logstash-%{+YYYY.MM.dd}" }
}
```

Kibana Visualization

- Visualize
- Dashboard
- Index Management



alert.signature.keyword: Descending	Count
ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	2
ET USER_AGENTS Win32.OnLineGames User-Agent (BigFoot)	1



event_type: alert

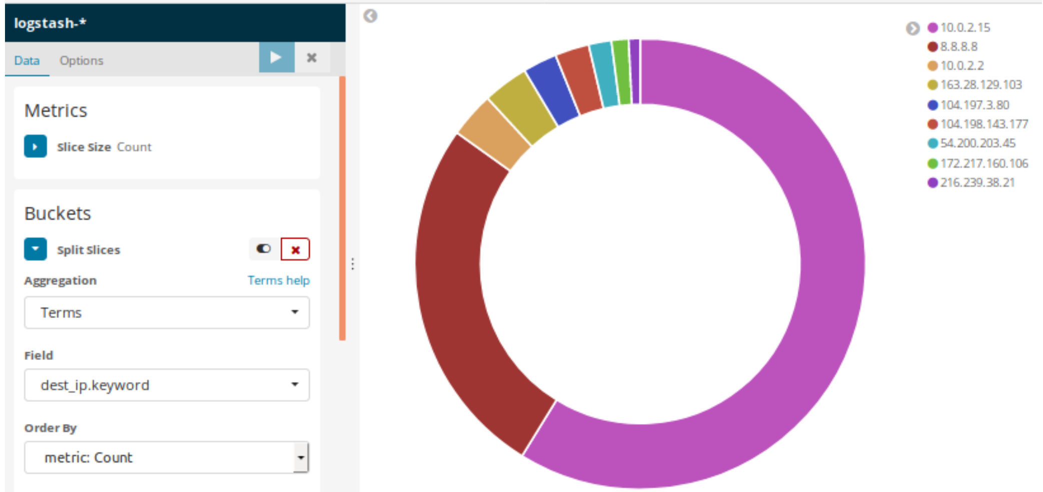
Metric Count

Split Rows alert.signature.keywo...

alert.signature.keyword: Descending
ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt

Lab2

- Kibana Visualizations
  - Top 10 Alert Signature
  - Top 10 source IP alerts
  - Top 10 destination IP alerts
  - Create a dashboard
  - Dashboard/Visualization Import



logstash-*

Data Options

Metrics

Slice Size Count

Buckets

Split Slices

Aggregation: Terms

Field: dest_ip.keyword

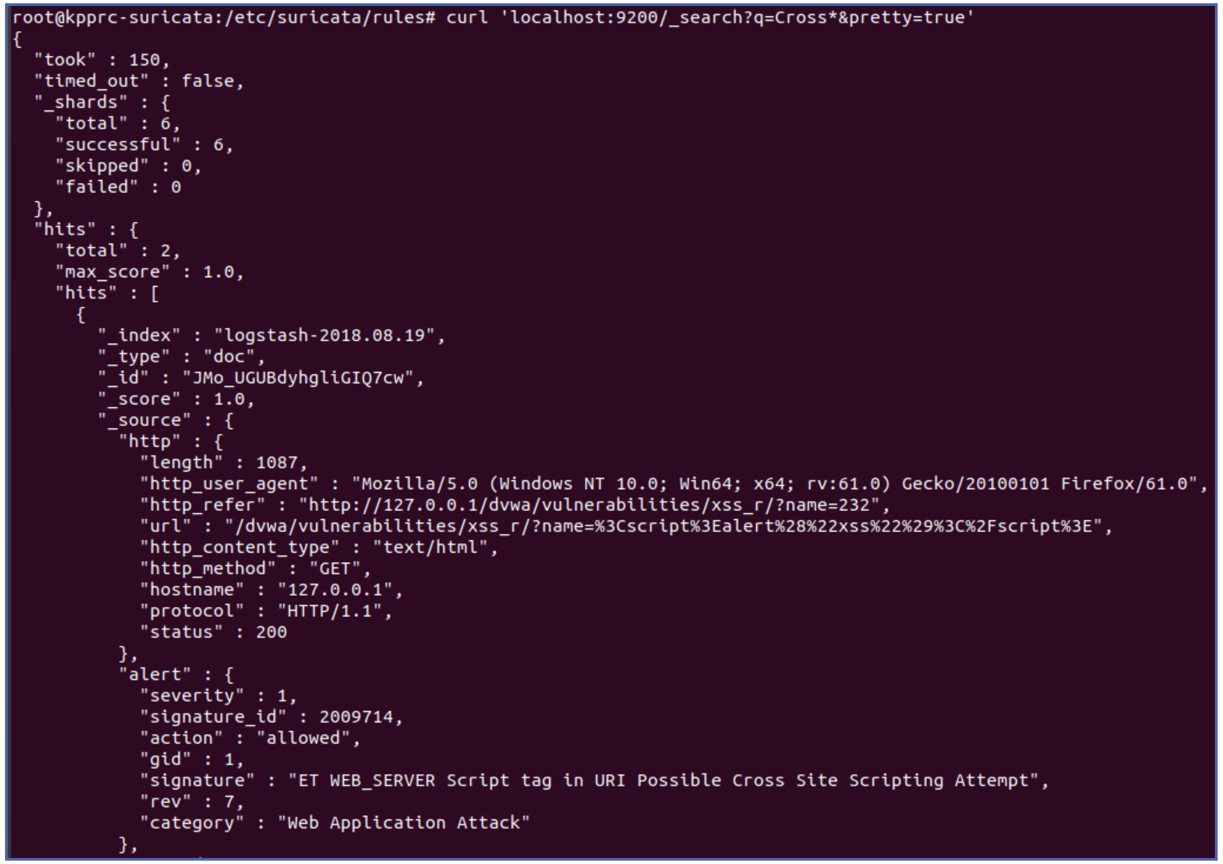
Order By: metric: Count

Elasticsearch query API (1/2)

- Syntax
  - http://ipaddress:port/index_name/type_name/_search?q=
- Simple Query Example
  - curl –XGET ‘localhost:9200/**logstash-2018-8-31/type_name**/_search?q=xss&pretty=true’ (index and type name)
  - curl –XGET ‘localhost:9200/**logstash-2018-8-31**/_search?q=xss&pretty=true’ (index name)
  - curl –XGET ‘localhost:9200/_search?q=xss&pretty=true’ (Search all index)

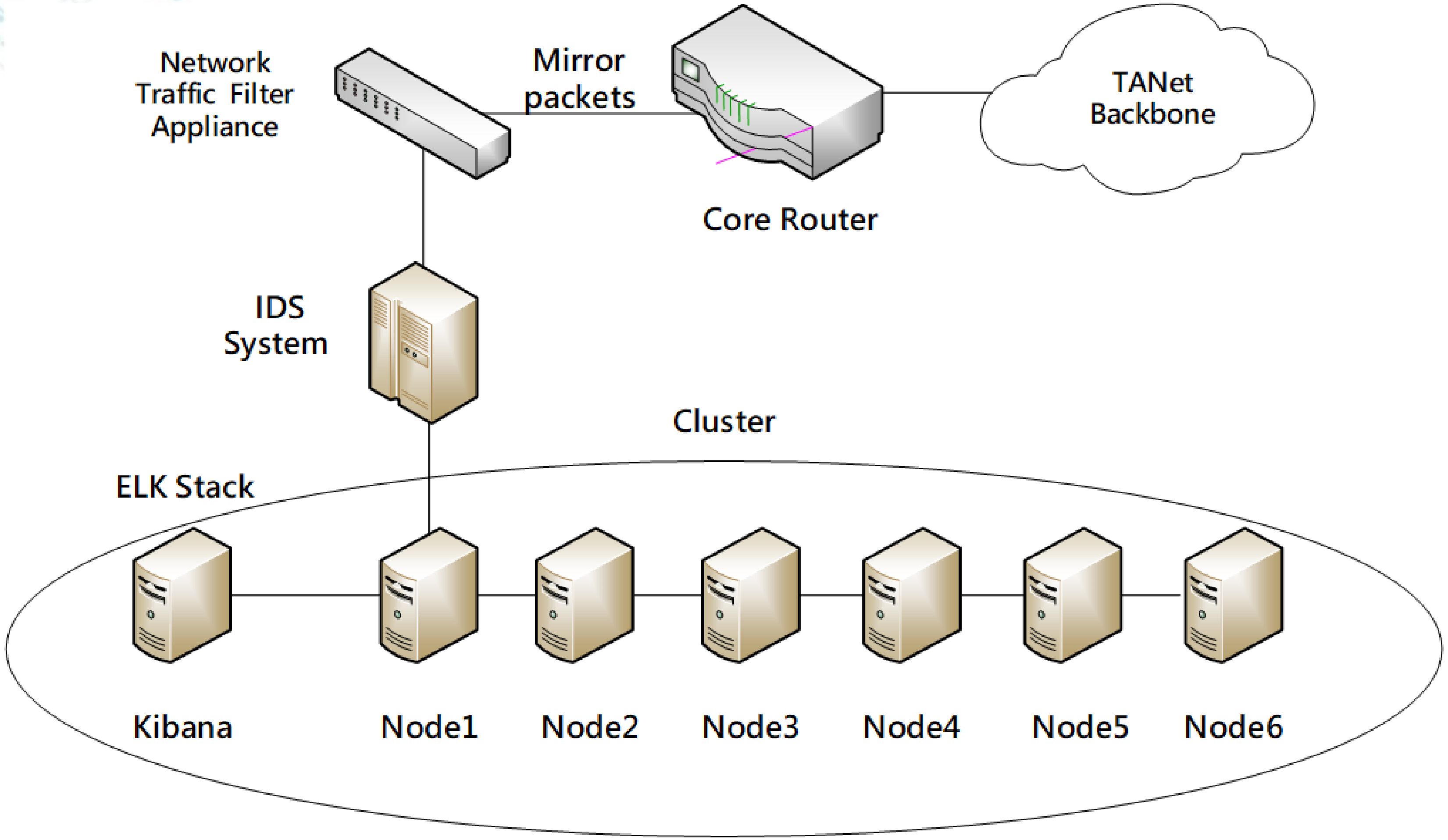
Elasticsearch query API (2/2)

- curl 'localhost:9200/_search?q=Cross*&pretty’
  - Search query string



```
root@kpprc-suricata:/etc/suricata/rules# curl 'localhost:9200/_search?q=Cross*&pretty=true'
{
  "took" : 150,
  "timed_out" : false,
  "_shards" : {
    "total" : 6,
    "successful" : 6,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : 2,
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "logstash-2018.08.19",
        "_type" : "doc",
        "_id" : "JMo_UGUBdyhgliGIQ7cw",
        "_score" : 1.0,
        "_source" : {
          "http" : {
            "length" : 1087,
            "http_user_agent" : "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0",
            "http_refer" : "http://127.0.0.1/dvwa/vulnerabilities/xss_r/?name=232",
            "url" : "/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22xss%22%29%3C%2Fscript%3E",
            "http_content_type" : "text/html",
            "http_method" : "GET",
            "hostname" : "127.0.0.1",
            "protocol" : "HTTP/1.1",
            "status" : 200
          },
          "alert" : {
            "severity" : 1,
            "signature_id" : 2009714,
            "action" : "allowed",
            "gid" : 1,
            "signature" : "ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt",
            "rev" : 7,
            "category" : "Web Application Attack"
          },
```

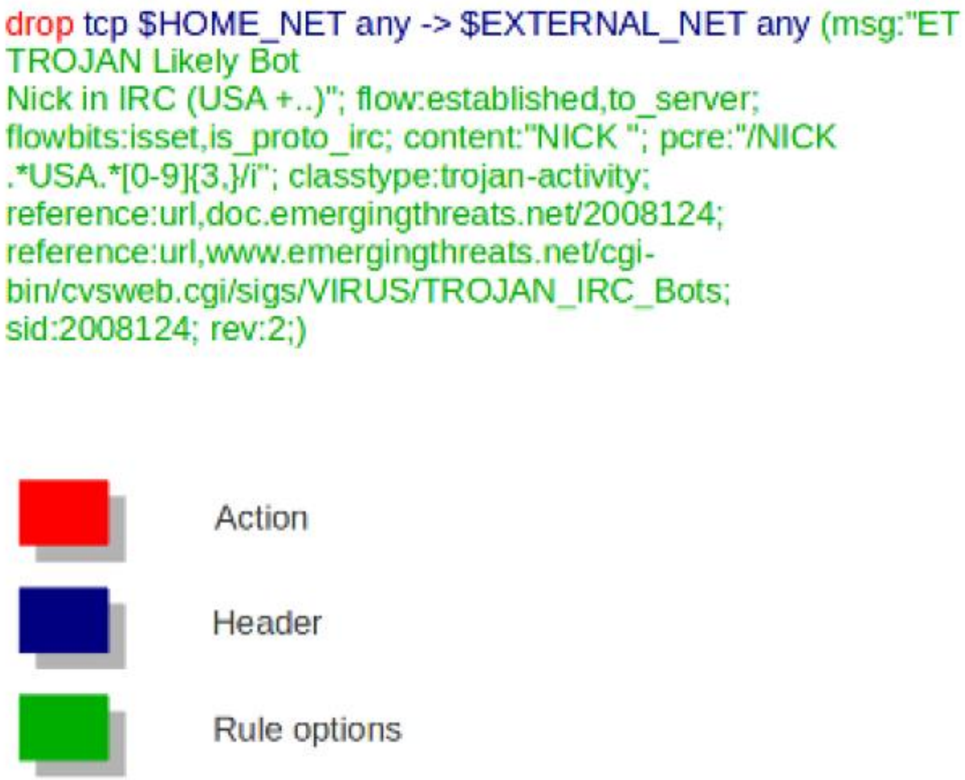
KPPRC IDS Architecture



Suricata偵測規則運作及探討

Suricata Rules

- PATH: /etc/suricata/rules



```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

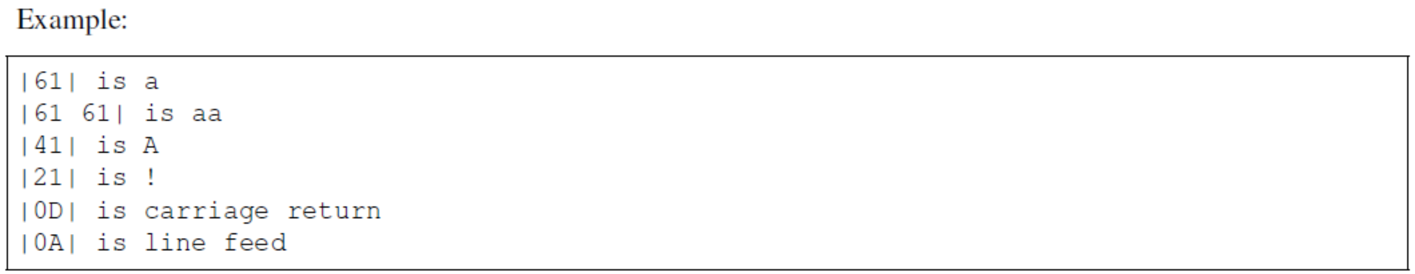
🟥 Action

🟦 Header

🟩 Rule options

Rule management

- Escape character: ; and “
  - msg:"Message with semicolon\;";
- 0x00 hex notation: |00|



Example:

```
|61| is a
|61 61| is aa
|41| is A
|21| is !
|0D| is carriage return
|0A| is line feed
```

- Character should use hex notation
- ” |22|
- ; |3B|
- : |3A|
- | |7C|
- content:“http|3A|//”

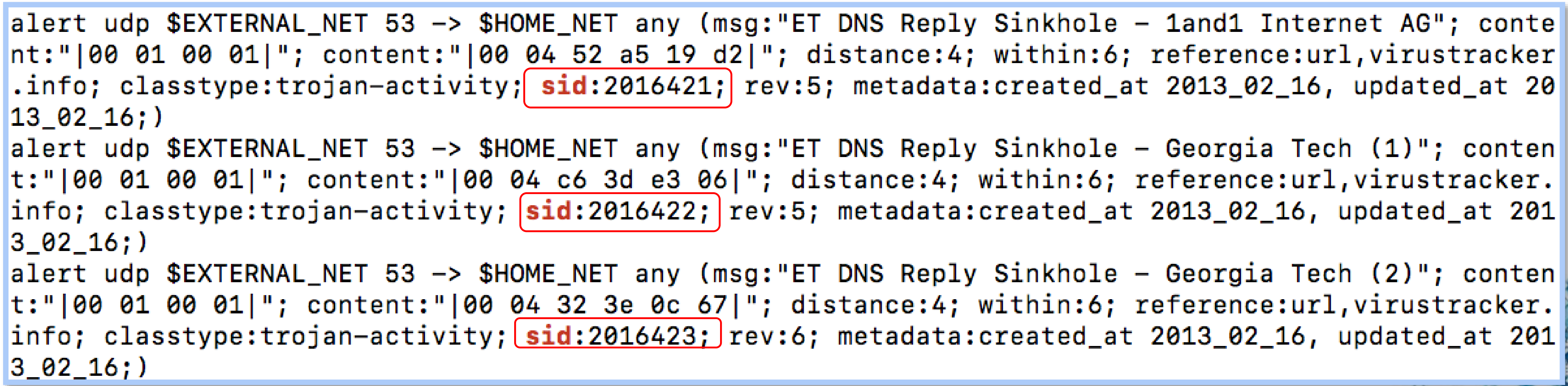
Meta Keywords

Keyword: **msg**

- msg(message) gives more information about the signature and the possible alert
- msg:"ET DOS Possible Cisco ASA 5500 Series Adaptive Security Appliance Remote SIP Inspection Device Reload Denial of Service Attempt";
- msg:"ET TOR Known Tor Exit Node Traffic group 6"

Keyword: **sid**

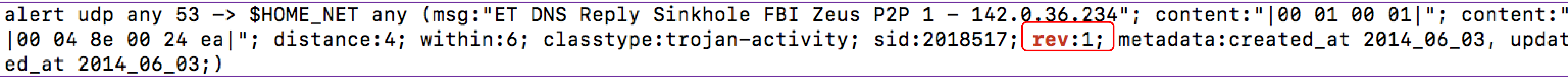
- sid (signature id)
  - gives every signature its own id
  - Number



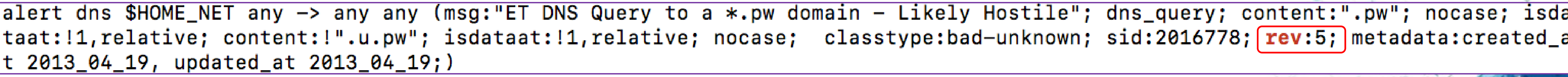
```
alert udp $EXTERNAL_NET 53 -> $HOME_NET any (msg:"ET DNS Reply Sinkhole - 1and1 Internet AG"; conte
nt:"|00 01 00 01|"; content:"|00 04 52 a5 19 d2|"; distance:4; within:6; reference:url,virustracker
.info; classtype:trojan-activity; sid:2016421; rev:5; metadata:created_at 2013_02_16, updated_at 20
13_02_16;)
alert udp $EXTERNAL_NET 53 -> $HOME_NET any (msg:"ET DNS Reply Sinkhole - Georgia Tech (1)"; conten
t:"|00 01 00 01|"; content:"|00 04 c6 3d e3 06|"; distance:4; within:6; reference:url,virustracker.
info; classtype:trojan-activity; sid:2016422; rev:5; metadata:created_at 2013_02_16, updated_at 201
3_02_16;)
alert udp $EXTERNAL_NET 53 -> $HOME_NET any (msg:"ET DNS Reply Sinkhole - Georgia Tech (2)"; conten
t:"|00 01 00 01|"; content:"|00 04 32 3e 0c 67|"; distance:4; within:6; reference:url,virustracker.
info; classtype:trojan-activity; sid:2016423; rev:6; metadata:created_at 2013_02_16, updated_at 201
3_02_16;)
```

Keyword: **rev**

- Rev(Revision): the version of the signature
- If a signature is modified, the number of rev will be incremented by the signature writers



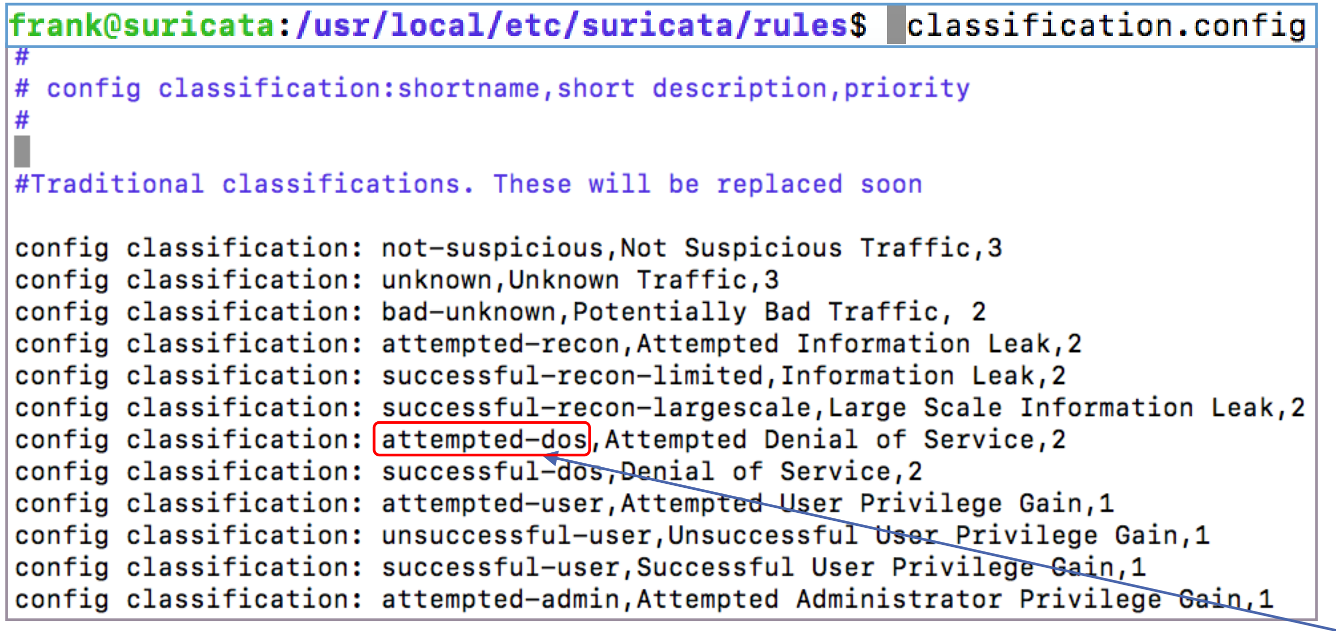
```
alert udp any 53 -> $HOME_NET any (msg:"ET DNS Reply Sinkhole FBI Zeus P2P 1 - 142.0.36.234"; content:"|00 01 00 01|"; content:"
|00 04 8e 00 24 ea|"; distance:4; within:6; classtype:trojan-activity; sid:2018517; rev:1; metadata:created_at 2014_06_03, updat
ed_at 2014_06_03;)
```



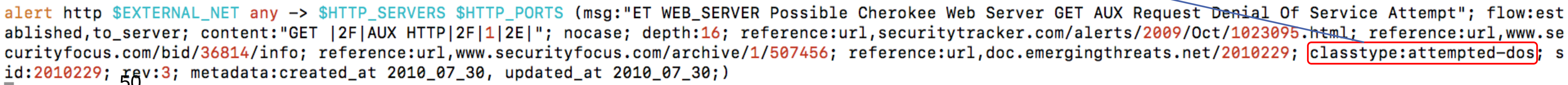
```
alert dns $HOME_NET any -> any any (msg:"ET DNS Query to a *.pw domain - Likely Hostile"; dns_query; content:".pw"; nocase; isda
taat:!1,relative; content:!".u.pw"; isdataat:!1,relative; nocase;  classtype:bad-unknown; sid:2016778; rev:5; metadata:created_a
t 2013_04_19, updated_at 2013_04_19;)
```

Keyword: **classtype**

- Gives information about the classification of rules and alerts
- It consists of a short name, short-description, and a priority



```
frank@suricata:/usr/local/etc/suricata/rules$  classification.config
#
# config classification:shortname,short description,priority
#

#Traditional classifications. These will be replaced soon

config classification: not-suspicious,Not Suspicious Traffic,3
config classification: unknown,Unknown Traffic,3
config classification: bad-unknown,Potentially Bad Traffic, 2
config classification: attempted-recon,Attempted Information Leak,2
config classification: successful-recon-limited,Information Leak,2
config classification: successful-recon-largescale,Large Scale Information Leak,2
config classification: attempted-dos,Attempted Denial of Service,2
config classification: successful-dos,Denial of Service,2
config classification: attempted-user,Attempted User Privilege Gain,1
config classification: unsuccessful-user,Unsuccessful User Privilege Gain,1
config classification: successful-user,Successful User Privilege Gain,1
config classification: attempted-admin,Attempted Administrator Privilege Gain,1
```

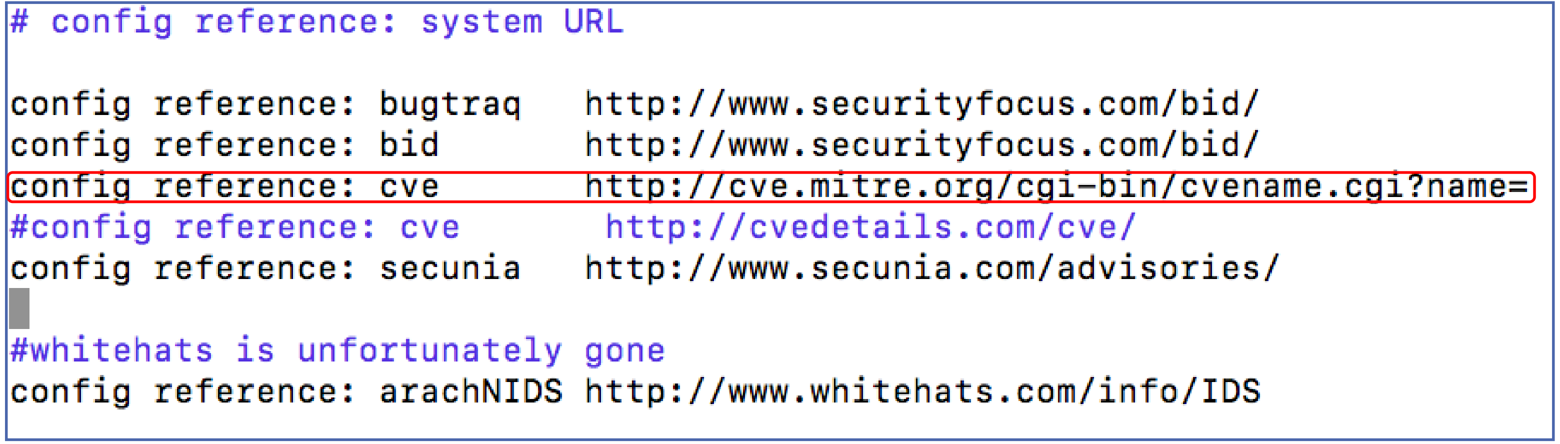


```
alert http $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET WEB_SERVER Possible Cherokee Web Server GET AUX Request Denial Of Service Attempt"; flow:est
ablished,to_server; content:"GET |2F|AUX HTTP|2F|1|2E|"; nocase; depth:16; reference:url,securitytracker.com/alerts/2009/Oct/1023095.html; reference:url,www.se
curityfocus.com/bid/36814/info; reference:url,www.securityfocus.com/archive/1/507456; reference:url,doc.emergingthreats.net/2010229; classtype:attempted-dos; s
id:2010229; rev:3; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
```

Keyword: **reference**

- Reference:
  - Information about the signature
  - reference: url, www.info.nl
  - 可參考 reference.config 檔案格式參考

reference.config



```
# config reference: system URL

config reference: bugtraq   http://www.securityfocus.com/bid/
config reference: bid       http://www.securityfocus.com/bid/
config reference: cve       http://cve.mitre.org/cgi-bin/cvename.cgi?name=
#config reference: cve       http://cvedetails.com/cve/
config reference: secunia   http://www.secunia.com/advisories/

#whitehats is unfortunately gone
config reference: arachNIDS http://www.whitehats.com/info/IDS
```

CVE編號格式

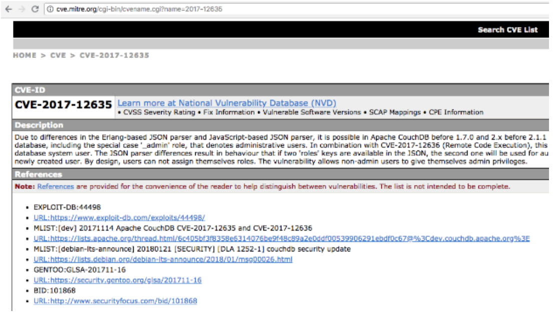
Keyword: **reference** (cont.)

- 實例解析

```
alert http any any -> $HOME_NET 5984 (msg:"ET EXPLOIT Apache CouchDB JSON Remote Prives
c Attempt (CVE-2017-12635)"; flow: established,to_server,only_stream; content:"PUT"; ht
tp_method; content:"/_users/"; content:"_admin"; http_client_body; fast_pattern; metada
ta: former_category EXPLOIT; reference:cve,2017-12635; reference:url,blog.trendmicro.co
m/trendlabs-security-intelligence/vulnerabilities-apache-couchdb-open-door-monero-miner
s/; classtype:attempted-admin; sid:2025435; rev:2; metadata:attack_target Server, deplo
yment Datacenter, signature_severity Major, created_at 2018_03_19, malware_family CoinM
iner, updated_at 2018_03_19;)
```

reference to

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-12635



cve.mitre.org/cgi-bin/cvename.cgi?name=2017-12635

Search CVE List

HOME > CVE > CVE-2017-12635

CVE-ID

CVE-2017-12635 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Due to differences in the Erlang-based JSON parser and JavaScript-based JSON parser, it is possible in Apache CouchDB before 1.7.0 and 2.x before 2.1.1
database, including the special case '_admin' role, that denotes administrative users. In combination with CVE-2017-12636 (Remote Code Execution), this
database system user. The JSON parser differences result in behaviour that if two 'roles' keys are available in the JSON, the second one will be used for au
newly created user. By design, users can not assign themselves roles. The vulnerability allows non-admin users to give themselves admin privileges.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB:44498
- URL:https://www.exploit-db.com/exploits/44498/
- MLIST:[dev] 20171114 Apache CouchDB CVE-2017-12635 and CVE-2017-12636
- URL:https://lists.apache.org/thread.html/6c405bf3f8358e6314076be9f48c89a2e0ddf00539906291ebdf0c67@%3Cdev.couchdb.apache.org%3E
- MLIST:[debian-lts-announce] 20180121 [SECURITY] [DLA 1252-1] couchdb security update
- URL:https://lists.debian.org/debian-lts-announce/2018/01/msg00026.html
- GENTOO:GLSA-201711-16
- URL:https://security.gentoo.org/glsa/201711-16
- BID:101868
- URL:http://www.securityfocus.com/bid/101868

Keyword: **priority**

- Range:1~255
- Most often used:1,2,3,4
- 數字愈低優先權愈高, Priority 1最高
- Signatures with a higher priority will be examined first

```
priority:1;
```

Keyword: **metadata** and **target**

- Metadata
  - Ignored by suricata
  - Compatible with signature language
  - 實例

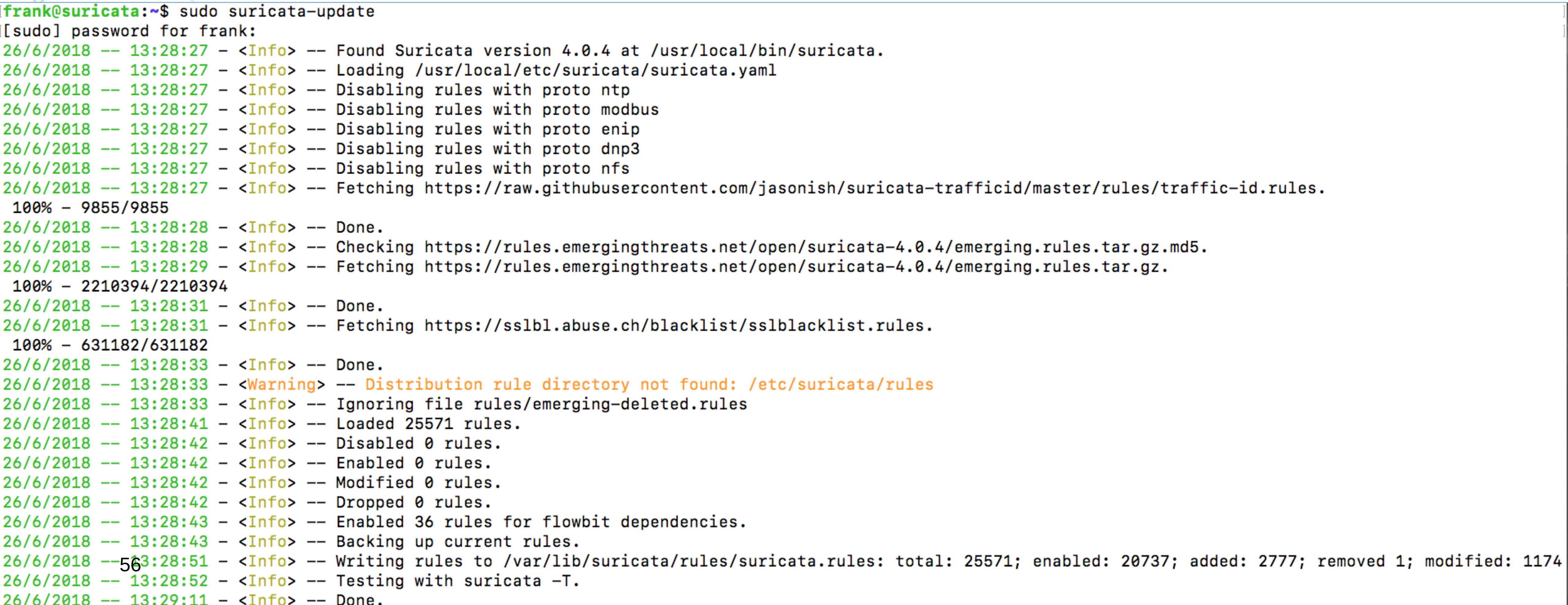
```
metadata:created_at 2014_02_18
```

- Target
  - specify which side of the alert is the target of the attack
  - Format, target:[src_ip|dest_ip]

Rule Management

Suricata-Update

- Use suricata-update command



```
frank@suricata:~$ sudo suricata-update
[sudo] password for frank:
26/6/2018 -- 13:28:27 - <Info> -- Found Suricata version 4.0.4 at /usr/local/bin/suricata.
26/6/2018 -- 13:28:27 - <Info> -- Loading /usr/local/etc/suricata/suricata.yaml
26/6/2018 -- 13:28:27 - <Info> -- Disabling rules with proto ntp
26/6/2018 -- 13:28:27 - <Info> -- Disabling rules with proto modbus
26/6/2018 -- 13:28:27 - <Info> -- Disabling rules with proto enip
26/6/2018 -- 13:28:27 - <Info> -- Disabling rules with proto dnp3
26/6/2018 -- 13:28:27 - <Info> -- Disabling rules with proto nfs
26/6/2018 -- 13:28:27 - <Info> -- Fetching https://raw.githubusercontent.com/jasonish/suricata-trafficid/master/rules/traffic-id.rules.
 100% - 9855/9855
26/6/2018 -- 13:28:28 - <Info> -- Done.
26/6/2018 -- 13:28:28 - <Info> -- Checking https://rules.emergingthreats.net/open/suricata-4.0.4/emerging.rules.tar.gz.md5.
26/6/2018 -- 13:28:29 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-4.0.4/emerging.rules.tar.gz.
 100% - 2210394/2210394
26/6/2018 -- 13:28:31 - <Info> -- Done.
26/6/2018 -- 13:28:31 - <Info> -- Fetching https://sslbl.abuse.ch/blacklist/sslblacklist.rules.
 100% - 631182/631182
26/6/2018 -- 13:28:33 - <Info> -- Done.
26/6/2018 -- 13:28:33 - <Warning> -- Distribution rule directory not found: /etc/suricata/rules
26/6/2018 -- 13:28:33 - <Info> -- Ignoring file rules/emerging-deleted.rules
26/6/2018 -- 13:28:41 - <Info> -- Loaded 25571 rules.
26/6/2018 -- 13:28:42 - <Info> -- Disabled 0 rules.
26/6/2018 -- 13:28:42 - <Info> -- Enabled 0 rules.
26/6/2018 -- 13:28:42 - <Info> -- Modified 0 rules.
26/6/2018 -- 13:28:42 - <Info> -- Dropped 0 rules.
26/6/2018 -- 13:28:43 - <Info> -- Enabled 36 rules for flowbit dependencies.
26/6/2018 -- 13:28:43 - <Info> -- Backing up current rules.
26/6/2018 -- 13:28:51 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 25571; enabled: 20737; added: 2777; removed 1; modified: 1174
26/6/2018 -- 13:28:52 - <Info> -- Testing with suricata -T.
26/6/2018 -- 13:29:11 - <Info> -- Done.
```

Suricata-Update (cont.)

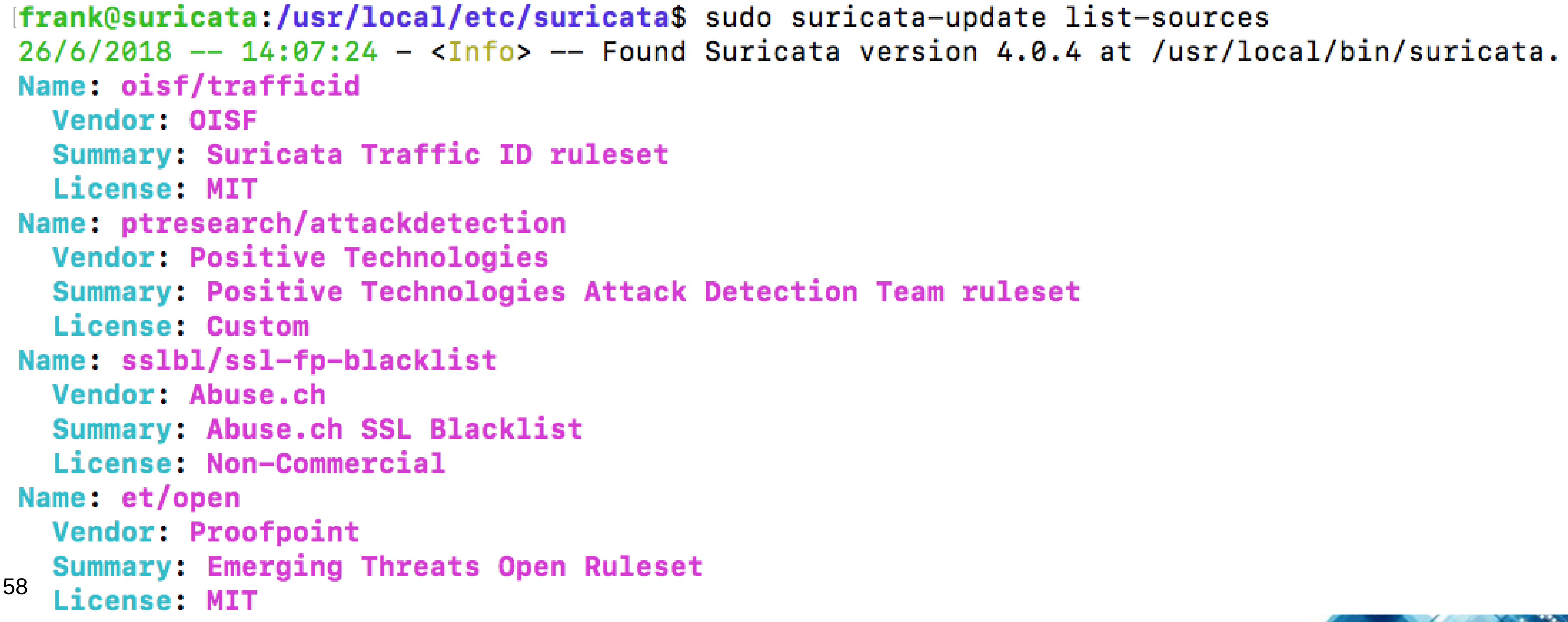
- Install
  - sudo apt install python-pip python-yaml
  - sudo pip install --pre --upgrade suricata-update
- Update rules
  - sudo suricata-update
  - Will merge all rules into **/var/lib/suricata/rules/suricata.rules** file
- Change configuration file as

filename: suricata.yaml

```
…
default-rule-path: /usr/local/etc/suricata/rules
 - suricata.rules
…
```

Suricata-Update (cont.)

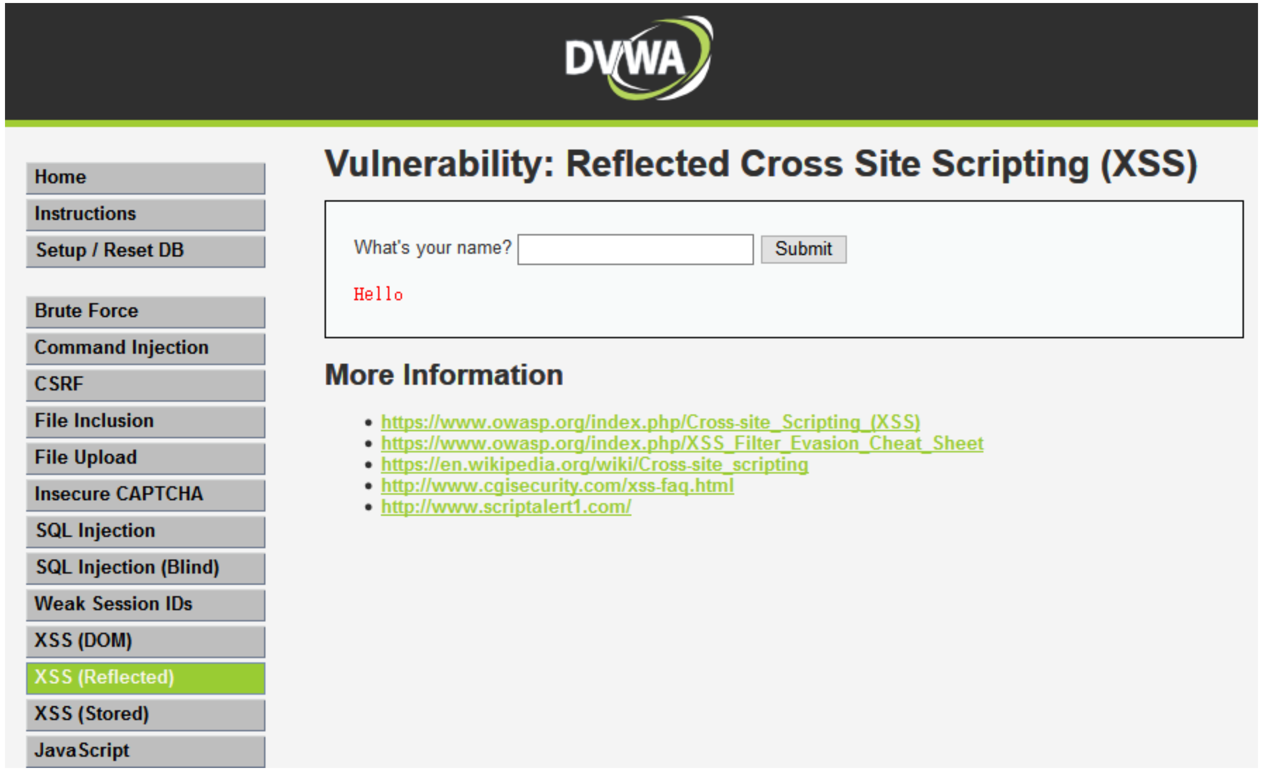
- Check what rules is available
  - suricata-update list-sources



```
[frank@suricata:/usr/local/etc/suricata$ sudo suricata-update list-sources
26/6/2018 -- 14:07:24 - <Info> -- Found Suricata version 4.0.4 at /usr/local/bin/suricata.
Name: oisf/trafficid
  Vendor: OISF
  Summary: Suricata Traffic ID ruleset
  License: MIT
Name: ptresearch/attackdetection
  Vendor: Positive Technologies
  Summary: Positive Technologies Attack Detection Team ruleset
  License: Custom
Name: sslbl/ssl-fp-blacklist
  Vendor: Abuse.ch
  Summary: Abuse.ch SSL Blacklist
  License: Non-Commercial
Name: et/open
  Vendor: Proofpoint
  Summary: Emerging Threats Open Ruleset
  License: MIT
```

DVWA

- DVWA - Damn Vulnerable Web Application
- Vulnerability Target



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

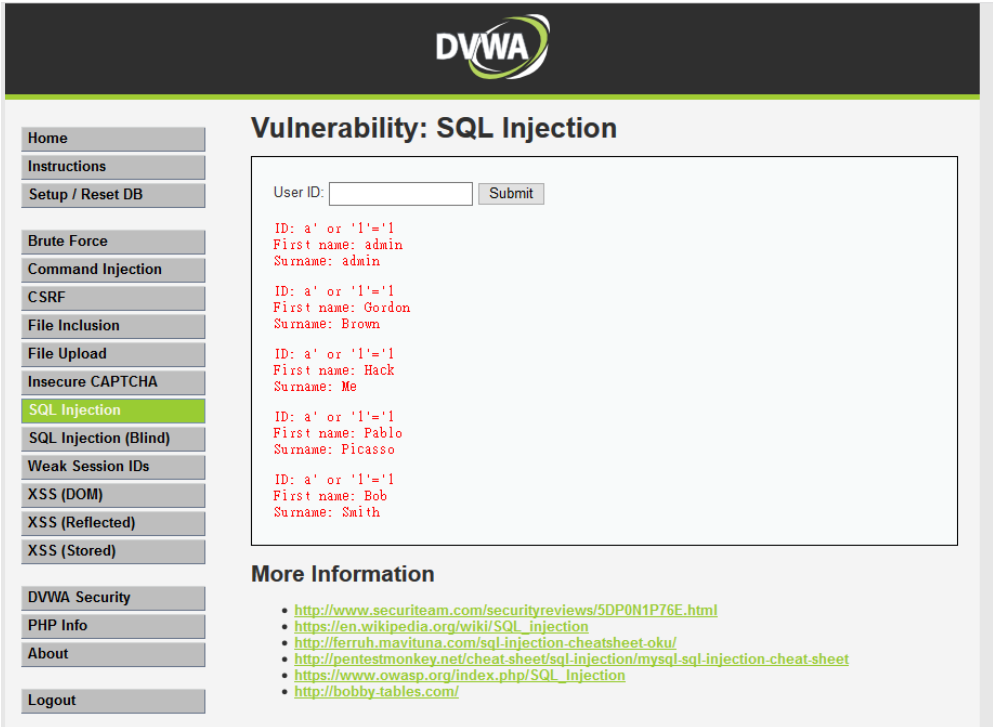
Hello

More Information

- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

Lab3

- DVWA
- Suricata Rule to detect SQL injection



Vulnerability: SQL Injection

User ID:

```
ID: a' or '1'='1
First name: admin
Surname: admin

ID: a' or '1'='1
First name: Gordon
Surname: Brown

ID: a' or '1'='1
First name: Hack
Surname: Me

ID: a' or '1'='1
First name: Pablo
Surname: Picasso

ID: a' or '1'='1
First name: Bob
Surname: Smith
```

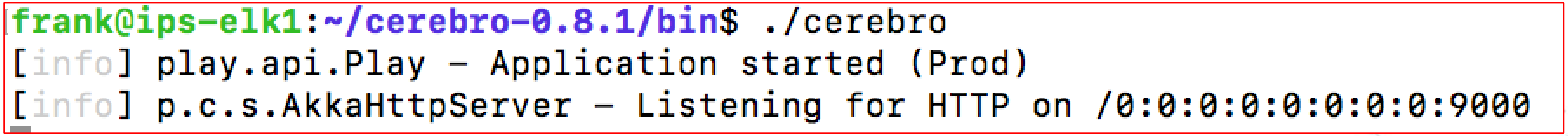
More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Trouble Shooting

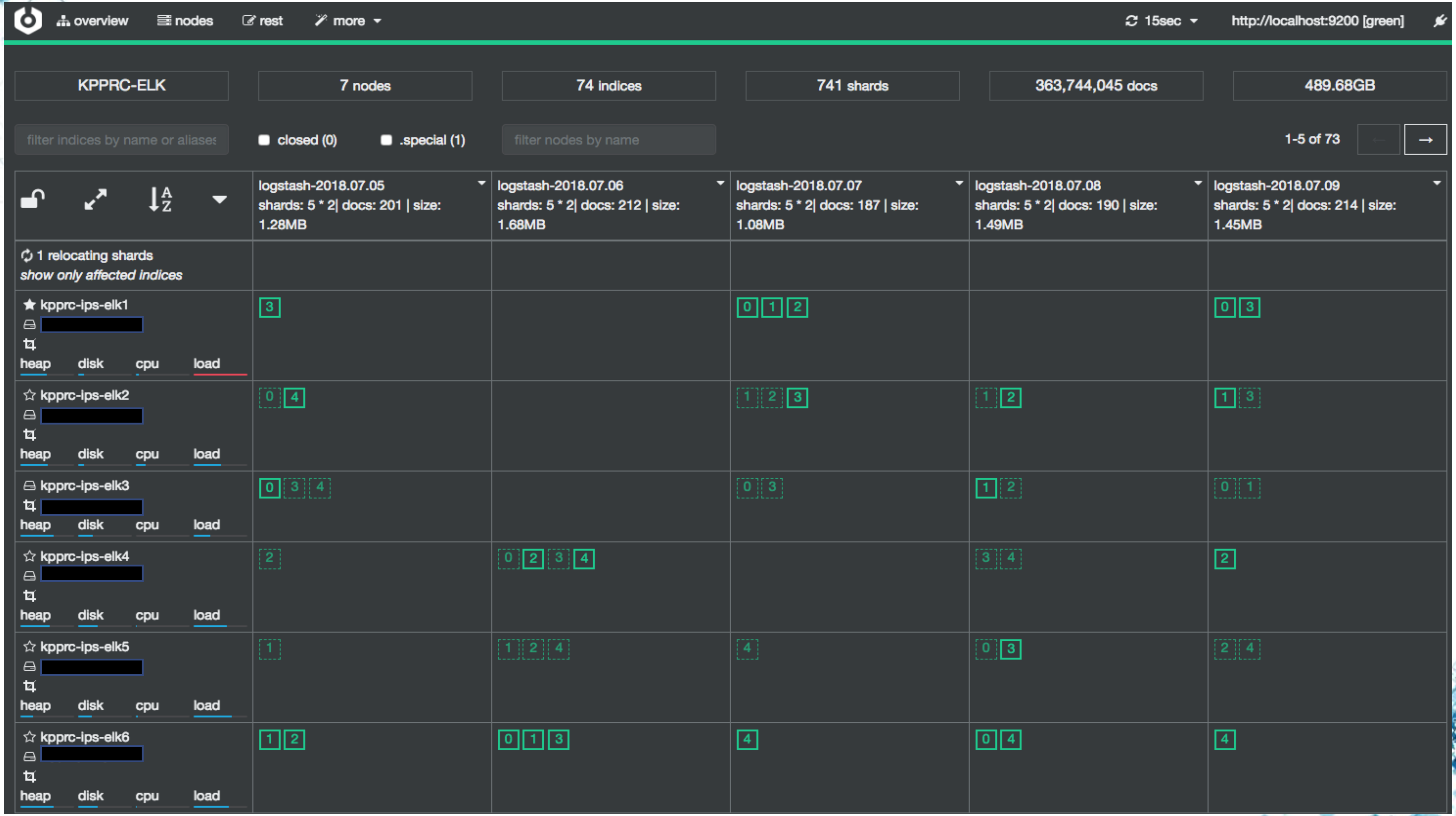
Cerebro Plugin

- Open source elasticsearch web admin tool
- Github page
  - https://github.com/lmenezes/cerebro
- Run bin/cerebro



```
frank@ips-elk1:~/cerebro-0.8.1/bin$ ./cerebro
[info] play.api.Play - Application started (Prod)
[info] p.c.s.AkkaHttpServer - Listening for HTTP on /0:0:0:0:0:0:0:0:9000
```

- Access on http://localhost:9000



KPPRC-ELK	7 nodes	74 indices	741 shards	363,744,045 docs	489.68GB

filter indices by name or aliases □ closed (0) □ .special (1) filter nodes by name 1-5 of 73 →

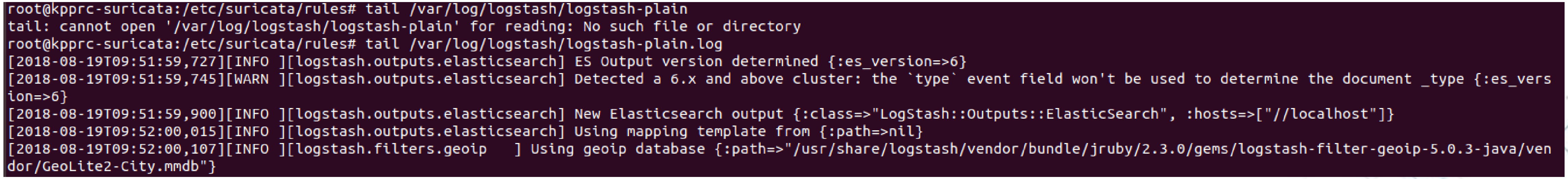
	logstash-2018.07.05 shards: 5 * 2| docs: 201 | size: 1.28MB	logstash-2018.07.06 shards: 5 * 2| docs: 212 | size: 1.68MB	logstash-2018.07.07 shards: 5 * 2| docs: 187 | size: 1.08MB	logstash-2018.07.08 shards: 5 * 2| docs: 190 | size: 1.49MB	logstash-2018.07.09 shards: 5 * 2| docs: 214 | size: 1.45MB
1 relocating shards *show only affected indices*					
★ kpprc-ips-elk1 [redacted] heap disk cpu load	3		0 1 2		0 3
☆ kpprc-ips-elk2 [redacted] heap disk cpu load	0 4		1 2 3	1 2	1 3
kpprc-ips-elk3 [redacted] heap disk cpu load	0 3 4		0 3	1 2	0 1
☆ kpprc-ips-elk4 [redacted] heap disk cpu load	2	0 2 3 4		3 4	2
☆ kpprc-ips-elk5 [redacted] heap disk cpu load	1	1 2 4	4	0 3	2 4
☆ kpprc-ips-elk6 [redacted] heap disk cpu load	1 2	0 1 3	4	0 4	4

Curl command

- Use curl command
  - cat APIs
- curl localhost:9200/_cat/indices?v
  - List all indexes
- curl localhost:9200/_cat/nodes?v
  - Shows the cluster topology
- curl -X GET "localhost:9200/_cluster/health?pretty=true"
  - Get cluster health
- Delete all index
  - curl -XDELETE localhost:9200/_all

Log files

- Elasticsearch
  - /var/log/elasticsearch
- Logstash
  - /var/log/logstash/



```
root@kpprc-suricata:/etc/suricata/rules# tail /var/log/logstash/logstash-plain
tail: cannot open '/var/log/logstash/logstash-plain' for reading: No such file or directory
root@kpprc-suricata:/etc/suricata/rules# tail /var/log/logstash/logstash-plain.log
[2018-08-19T09:51:59,727][INFO ][logstash.outputs.elasticsearch] ES Output version determined {:es_version=>6}
[2018-08-19T09:51:59,745][WARN ][logstash.outputs.elasticsearch] Detected a 6.x and above cluster: the `type` event field won't be used to determine the document _type {:es_vers
ion=>6}
[2018-08-19T09:51:59,900][INFO ][logstash.outputs.elasticsearch] New Elasticsearch output {:class=>"LogStash::Outputs::ElasticSearch", :hosts=>["//localhost"]}
[2018-08-19T09:52:00,015][INFO ][logstash.outputs.elasticsearch] Using mapping template from {:path=>nil}
[2018-08-19T09:52:00,107][INFO ][logstash.filters.geoip   ] Using geoip database {:path=>"/usr/share/logstash/vendor/bundle/jruby/2.3.0/gems/logstash-filter-geoip-5.0.3-java/ven
dor/GeoLite2-City.mmdb"}
```

Reference

- https://github.com/OISF/suricata
- https://suricata.readthedocs.io/en/suricata-4.0.5/install.html
- https://media.readthedocs.org/pdf/suricata/latest/suricata.pdf