Suricata 2.0, Netfilter and the PRC

Éric Leblond

Stamus Networks

July 8, 2014

STAMUS NETWORKS

Eric Leblond a.k.a Regit

- French
- Network security expert
- Free Software enthousiast
- NuFW project creator (Now ufwi), EdenWall co-founder
- Netfilter developer:
  - Maintainer of ulogd2: Netfilter logging daemon
  - Misc contributions:
    - NFQUEUE library and associates
    - Port of some features iptables to nftables
- Currently:
  - co-founder of Stamus Networks, a company providing Suricata based network probe appliances.
  - Suricata IDS/IPS funded developer

STAMUS NETWORKS

STAMUS NETWORKS

STAMUS NETWORKS

What is Suricata

- IDS and IPS engine
- Get it here:
  `http://www.suricata-ids.org`
- Open Source (GPLv2)
- Funded by US government and consortium members
- Run by Open Information Security Foundation (OISF)
- More information about OISF at
  `http://www.openinfosecfoundation.org/`

STAMUS NETWORKS

Suricata Features

- High performance, scalable through multi threading
- Protocol identification
- File identification, extraction, on the fly MD5 calculation
- TLS handshake analysis, detect/prevent things like Diginotar
- Hardware acceleration support:
  - Endace
  - Napatech,
  - CUDA
  - PF_RING

STAMUS NETWORKS

Suricata Features

- Rules and outputs compatible to Snort syntax
- useful logging like HTTP request log, TLS certificate log, DNS logging
- Lua scripting for detection

STAMUS NETWORKS

Suricata capture modes

IDS

- pcap: multi OS capture
- pf_ring: Linux high performance
- af_packet: Linux high performance on vanilla kernel
- ...

IPS

- NFQUEUE: Using Netfilter on Linux
- ipfw: Use divert socket on FreeBSD
- af_packet: Level 2 software bridge

Offline analysis

- Pcap: Analyse pcap files
- Unix socket: Use Suricata for fast batch processing of pcap files

Suricata 2.0 new features

- ’EVE’ logging, our all JSON output for events: alerts, HTTP, DNS, SSH, TLS and (extracted) files
- much improved VLAN handling
- a detectionless ‘NSM’ runmode
- much improved CUDA performance

STAMUS NETWORKS

STAMUS NETWORKS

STAMUS NETWORKS

Let's get rid of the 90's

Let's kill unified2

- Binary format without real design
- Dedicated to alert
- Very hard to extend
- No API on devel side

We need something extensible

- To log alert and to log protocol request
- Easy to generate and easy to parse
- Extensible

STAMUS NETWORKS

JavaScript Object Notation

JSON

- JSON (`http://www.json.org/`) is a lightweight data-interchange format.
- It is easy for humans to read and write.
- It is easy for machines to parse and generate.
- An object is an unordered set of name/value pairs.

Logging in JSON

```
{"timestamp":"2012-02-05T15:55:06.661269", "src_ip":"173.194.34.51",
 "dest_ip":"192.168.1.22",
 "alert":{"action":"allowed",rev":1,"signature":"SURICATA TLS store"}}
```

STAMUS NETWORKS

Alert

The structure

- IP information are identical for all events and alert
- Follow Common Information Model
- Allow basic aggregation for all Suricata events and external sources

Example

```
{"timestamp":"2014-03-06T05:46:31.170567","event_type":"alert",
 "src_ip":"61.174.51.224","src_port":2555,
 "dest_ip":"192.168.1.129","dest_port":22,"proto":"TCP",
 "alert":{"action":"Pass","gid":1,"signature_id":2006435,"rev":8,
          "signature":"ET SCAN LibSSH Based SSH Connection - Often used as
          "category":"Misc activity","severity":3}
}
```

STAMUS NETWORKS

Network Security Monitoring

Protocols

- HTTP
- File
- TLS
- SSH
- DNS

Example


```
{"timestamp":"2014-04-10T13:26:05.500472","event_type":"ssh",
 "src_ip":"192.168.1.129","src_port":45005,
 "dest_ip":"192.30.252.129","dest_port":22,"proto":"TCP",
 "ssh":{
  "client":{
    "proto_version":"2.0","software_version":"OpenSSH_6.6p1 Debian-2" },
  "server":{
    "proto_version":"2.0","software_version":"libssh-0.6.3"}
 }
}
```

STAMUS NETWORKS

At the beginning was syslog

Pre Netfilter days

- Flat packet logging
- One line per packet
  - A lot of information
  - Non searchable

STAMUS NETWORKS

At the beginning was syslog

Pre Netfilter days

- Flat packet logging
- One line per packet
  - A lot of information
  - Non searchable

Not sexy

```
INPUT DROP IN=eth0 OUT= MAC=00:1a:92:05:ee:68:00:b0:8e:83:3b:f0:08:00 SRC=62.212.121.211 DST=91.12
IN IN=eth0 OUT= MAC=d4:be:d9:69:d1:51:00:11:95:63:c7:5e:08:00 SRC=31.13.80.7 DST=192.168.11.3 LEN=
IN IN=eth0 OUT= MAC=d4:be:d9:69:d1:51:00:11:95:63:c7:5e:08:00 SRC=31.13.80.23 DST=192.168.11.3 LEN
IN IN=eth0 OUT= MAC=d4:be:d9:69:d1:51:00:11:95:63:c7:5e:08:00 SRC=31.13.80.7 DST=192.168.11.3 LEN=
IN IN=eth0 OUT= MAC=d4:be:d9:69:d1:51:00:11:95:63:c7:5e:08:00 SRC=31.13.80.7 DST=192.168.11.3 LEN=
```

STAMUS NETWORKS

Ulogd2: complete Netfilter logging

Ulogd2

- Interact with the post 2.6.14 libraries
- multiple output and input through the use of stacks

libnetfilter_log (generalized ulog)

- Packet logging
- IPv6 ready
- Few structural modification

libnetfilter_conntrack (new)

- Connection tracking logging
- Accounting, logging

libnetfilter_nfacct (added recently)

- High performance accounting

Ulogd: output and configuration

Sexify output

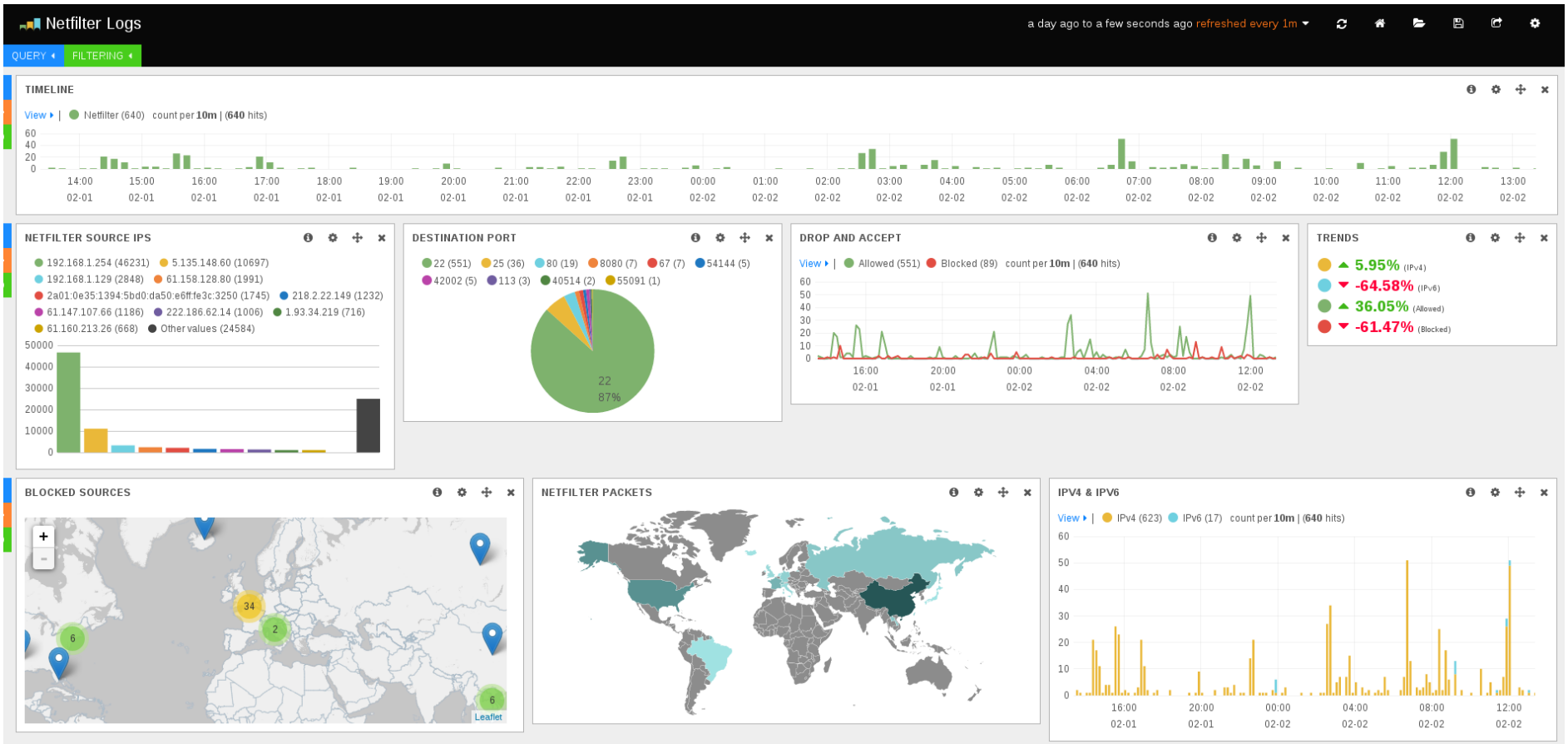
- Syslog and file output
- SQL output: PGSQL, MySQL, SQLite
- Graphite
- JSON output

Some stack examples

```
stack=log2:NFLOG,base1:BASE,ifi1:IFINDEX, \
      ip2str1:IP2STR,mac2str1:HWHDR,json1:JSON
stack=ct1:NFCT,mark1:MARK,ip2str1:IP2STR,pgsql2:PGSQL
```

STAMUS NETWORKS

Ulogd



STAMUS NETWORKS

STAMUS NETWORKS

ELK

- Elasticsearch is a distributed restful search and analytics
- Full text search, schema free
- Apache 2 open source license
- ELK stack
  - Elasticsearch
  - Logstash: log shipping
  - Kibana: web interface

STAMUS NETWORKS

Logstash

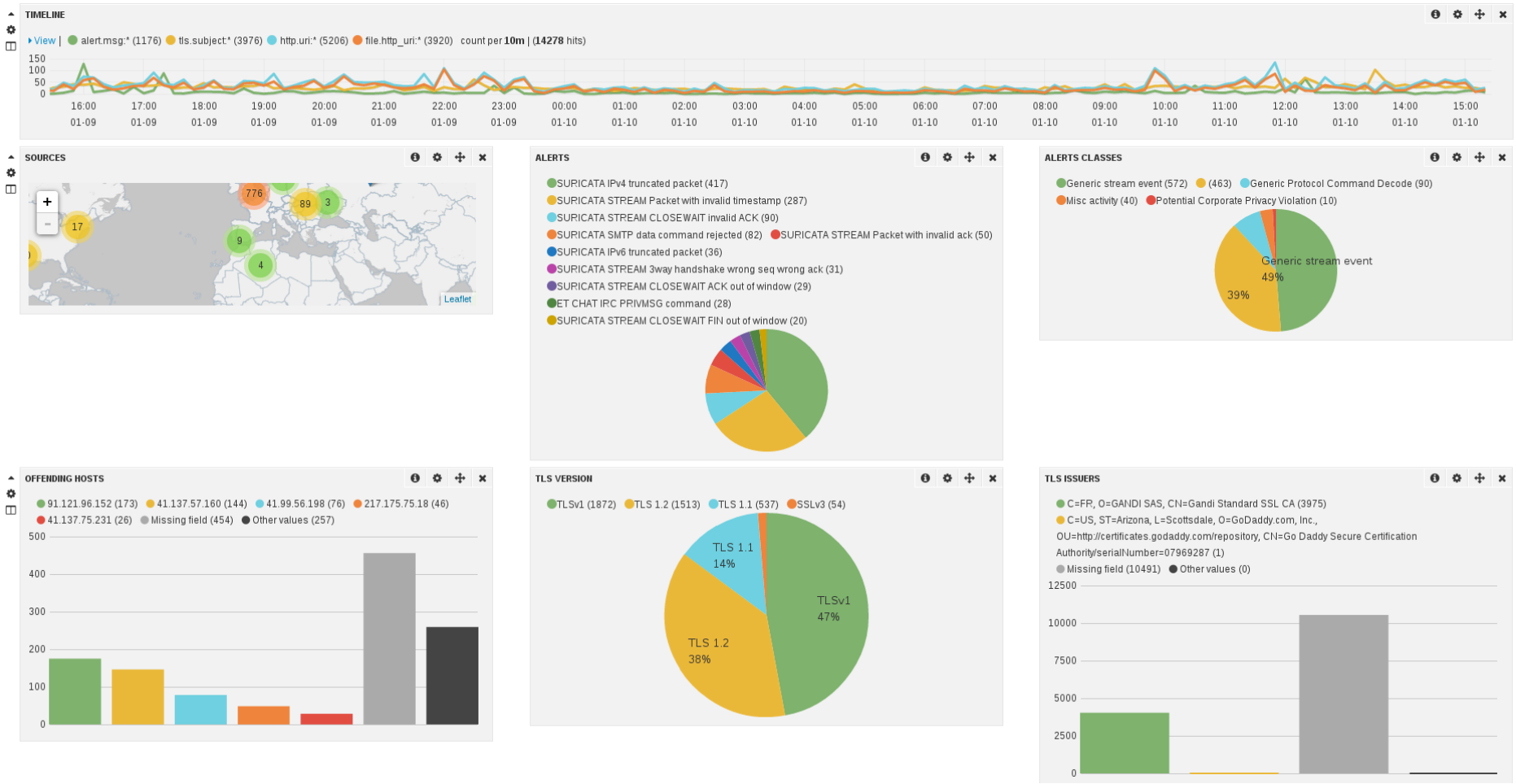
A tool for managing events and logs

- collect logs, parse them, and store them in different outputs
  - elasticsearch
  - graphite
  - IRC
  - ...
- Apache 2.0 license
-

A simple configuration (for JSON)

```
input {
   file {
      path => [ "/var/log/suricata/eve.json", "/var/log/ulogd.json"]
      codec =>   json
   }
}
```

Kibana


TIMELINE
View | alert.msg:* (1176) tls.subject:* (3976) http.uri:* (5206) file.http_uri:* (3920) count per 10m | (14278 hits)
150
100
50
0
16:00 01-09
17:00 01-09
18:00 01-09
19:00 01-09
20:00 01-09
21:00 01-09
22:00 01-09
23:00 01-09
00:00 01-10
01:00 01-10
02:00 01-10
03:00 01-10
04:00 01-10
05:00 01-10
06:00 01-10
07:00 01-10
08:00 01-10
09:00 01-10
10:00 01-10
11:00 01-10
12:00 01-10
13:00 01-10
14:00 01-10
15:00 01-10
SOURCES
776
89
3
17
9
4
Leaflet
ALERTS
SURICATA IPv4 truncated packet (417)
SURICATA STREAM Packet with invalid timestamp (287)
SURICATA STREAM CLOSEWAIT invalid ACK (90)
SURICATA SMTP data command rejected (82)
SURICATA STREAM Packet with invalid ack (50)
SURICATA IPv6 truncated packet (36)
SURICATA STREAM 3way handshake wrong seq wrong ack (31)
SURICATA STREAM CLOSEWAIT ACK out of window (29)
ET CHAT IRC PRIVMSG command (28)
SURICATA STREAM CLOSEWAIT FIN out of window (20)
ALERTS CLASSES
Generic stream event (572)
(463)
Generic Protocol Command Decode (90)
Misc activity (40)
Potential Corporate Privacy Violation (10)
Generic stream event
49%
39%
OFFENDING HOSTS
91.121.96.152 (173)
41.137.57.160 (144)
41.99.56.198 (76)
217.175.75.18 (46)
41.137.75.231 (26)
Missing field (454)
Other values (257)
500
400
300
200
100
0
TLS VERSION
TLSv1 (1872)
TLS 1.2 (1513)
TLS 1.1 (537)
SSLv3 (54)
TLS 1.1
14%
TLSv1
47%
TLS 1.2
38%
TLS ISSUERS
C=FR, O=GANDI SAS, CN=Gandi Standard SSL CA (3975)
C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certificates.godaddy.com/repository, CN=Go Daddy Secure Certification Authority/serialNumber=07969287 (1)
Missing field (10491)
Other values (0)
12500
10000
7500
5000
2500
0

STAMUS NETWORKS

Plotting TCP window at start

OS passive fingerprinting

- Value of TCP window at start is not specified in RFC
- The value is a choice of the OS
- We can use this for identification

Value for some OSes

- 8192: Windows 7 SP1
- 65535: Mac OS X 10.2 - 10.7
- 14600: Some Linux
- 5840: Some other Linux

Source: `http://noc.to/#Help:TcpSynPacketSignature`

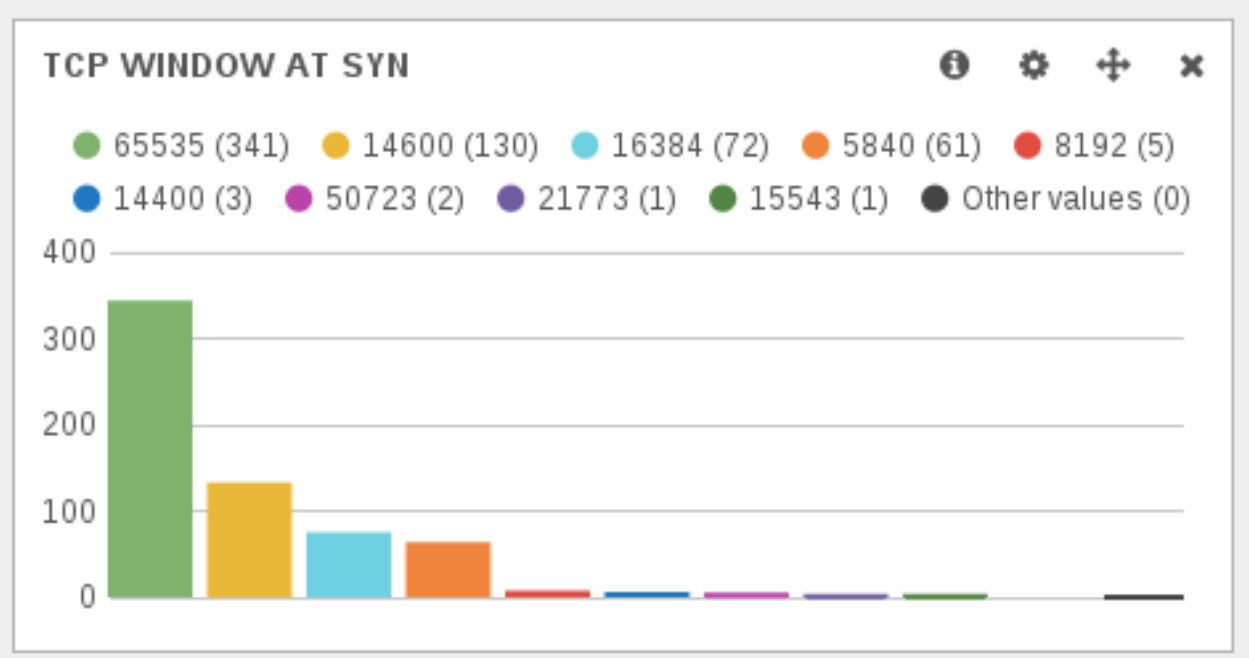
STAMUS NETWORKS

Demonstration

Let's pray Murphy

STAMUS NETWORKS

The facts



STAMUS NETWORKS

The facts

The facts

@timestamp	src_ip	src_port	dest_port
2014-02-02T12:58:11.735Z	61.174.51.219	6000	22
2014-02-02T12:55:24.699Z	222.186.62.20	6000	22
2014-02-02T12:49:04.621Z	222.186.62.42	6000	22
2014-02-02T12:28:28.150Z	222.186.62.53	6000	22
2014-02-02T12:26:02.045Z	61.160.195.250	6000	22
2014-02-02T12:21:00.961Z	61.160.215.5	6000	22
2014-02-02T11:45:40.916Z	61.174.51.201	6000	22
2014-02-02T11:44:09.874Z	115.230.126.87	6000	22

STAMUS NETWORKS

The facts

@timestamp	src_ip	src_port	dest_port	geoip.country_name	tcp.window
2014-01-31T08:11:15.314Z	61.160.223.102	6000	22	China	16384
2014-01-31T08:19:16.371Z	61.160.223.102	4585	22	China	65535
2014-01-31T08:20:08.378Z	61.160.223.102	1901	22	China	65535
2014-01-31T08:20:35.381Z	61.160.223.102	2363	22	China	65535
2014-01-31T08:20:44.383Z	61.160.223.102	2919	22	China	65535
2014-01-31T08:20:57.385Z	61.160.223.102	1208	22	China	65535
2014-01-31T08:21:07.387Z	61.160.223.102	4382	22	China	65535
2014-01-31T08:21:30.390Z	61.160.223.102	4519	22	China	65535
2014-01-31T08:21:51.393Z	61.160.223.102	4219	22	China	65535
2014-01-31T08:22:13.396Z	61.160.223.102	3548	22	China	65535
2014-01-31T08:22:33.399Z	61.160.223.102	1798	22	China	65535
2014-01-31T08:22:55.402Z	61.160.223.102	1275	22	China	65535
2014-02-02T10:56:04.435Z	61.160.223.102	6000	22	China	16384
2014-02-02T11:04:29.575Z	61.160.223.102	4075	22	China	65535
2014-02-02T11:04:52.582Z	61.160.223.102	4793	22	China	65535

STAMUS NETWORKS

STAMUS NETWORKS

Don’t forget the French hospitality

Interaction is limited

- Suricata just have the user agent
- Syslog just give the username
- We don’t have the used passwords
- We need to trap the offenders

How can we identify them ?


```
{"timestamp":"2014-04-10T13:26:05.500472","event_type":"ssh",
 "src_ip":"192.168.1.129","src_port":45005,
 "dest_ip":"192.30.252.129","dest_port":22,"proto":"TCP",
 "ssh":{
  "client":{
    "proto_version":"2.0","software_version":"OpenSSH_6.6p1 Debian-2" },
  "server":{
    "proto_version":"2.0","software_version":"libssh-0.6.3"}
 }
}
```

Let's build a honeypot

- Parse EVE JSON file to get user with interesting client version
- Add them to an IPSET set
- Redirect all IP in the IPPSET set to a honeypot
- Get info from fake server
- Store them in Elasticsearch

STAMUS NETWORKS

Deny On Monitoring: simple code

Principle

- Parse EVE JSON file (like tail)
- Check for client version
- Call the ipset command if the version is matching given string

Get it

- Written in Python
- Available under GPLv3
- Hosted on github: `https://github.com/regit/DOM`

STAMUS NETWORKS

Deny On Monitoring: simple code

```
def main_task(args):
    setup_logging(args)
    file = open(args.file, 'r')
    while 1:
        where = file.tell()
        line = file.readline()
        if not line:
            # Dodo
            time.sleep(0.3)
            file.seek(where)
        else:
            try:
                event = json.loads(line)
            except json.decoder.JSONDecodeError:
                time.sleep(0.3)
                break
            if event['event_type'] == 'ssh':
                if 'libssh' in event['ssh']['client']['software_version']:
                    # Vas-y Francis, c'est bon bon bon
                    call([IPSET, 'add', args.ipset, event['src_ip']])
```

STAMUS NETWORKS

Deny On Monitoring

Some users feedback

Deny On Monitoring

Some users feedback

Dom is one of the key protection of IMF network.

Christine Lagarde

Deny On Monitoring

Some users feedback

Dom is one of the key protection of IMF network.

Christine Lagarde

Dom, c'est vraiment bien contre le scan de porc.

Marcela Lacub

Deny On Monitoring

Some users feedback

Dom is one of the key protection of IMF network.

Christine Lagarde

Dom, c'est vraiment bien contre le scan de porc.

Marcela Lacub

Dom, y nique trop de scans!

Dodo la saumure

pshiit

Passwords of SSH Intruders Transferred to Text

- Fake SSH server
- Write username and password tried in a file using JSON format

Get it

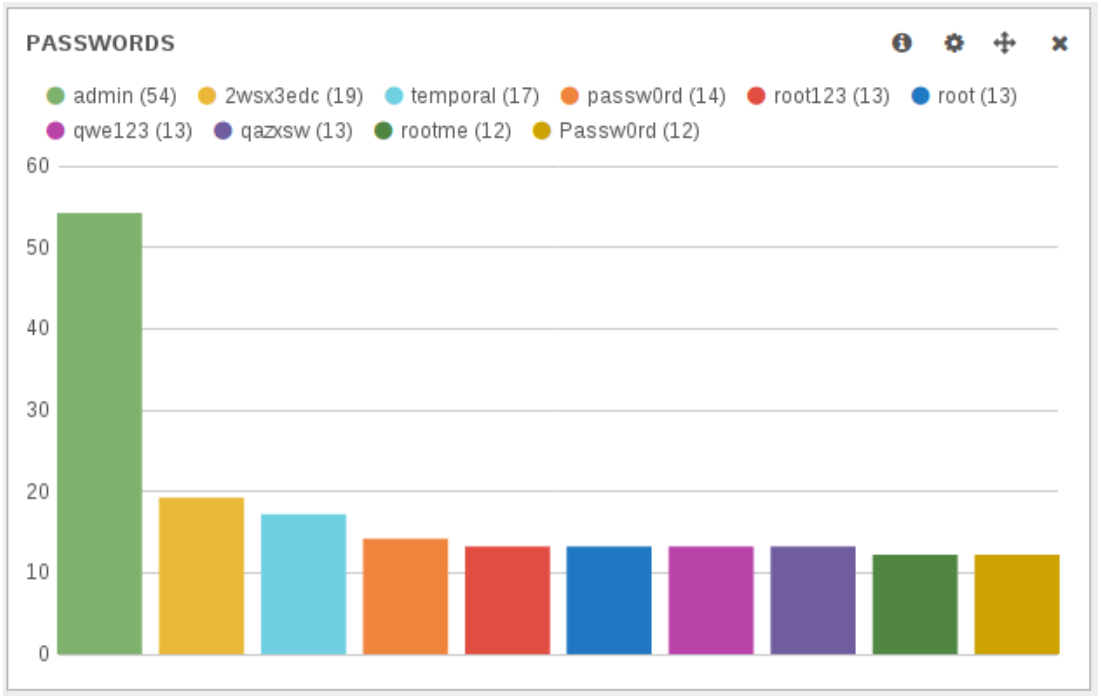
- Written in Python
- Use paramiko for SSH part
- Available under GPLv3
- Hosted on github: `https://github.com/regit/pshitt`

STAMUS NETWORKS

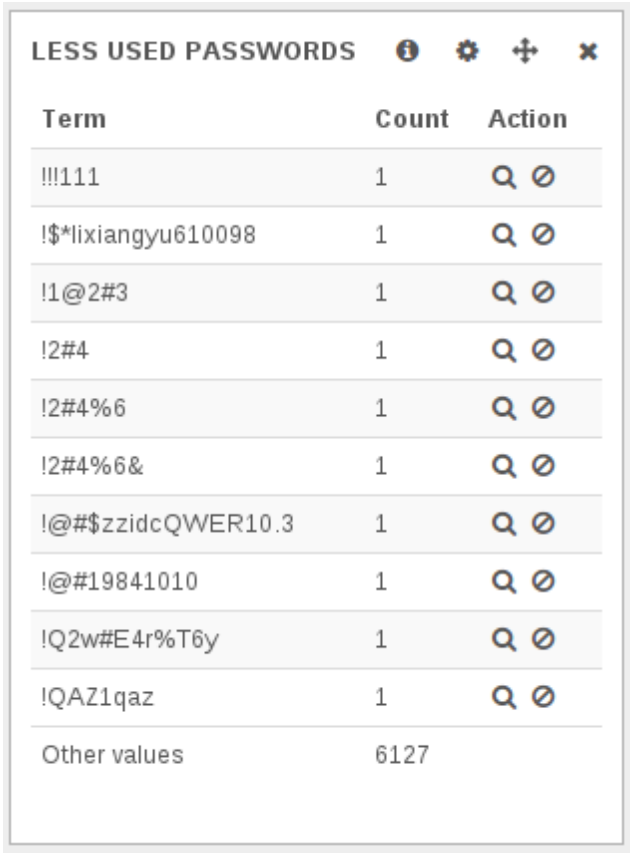
The complete setup

```
# create IPSET set
ipset create libssh hash:ip
# start DOM to populate set
cd DOM
./dom -f /usr/local/var/log/suricata/eve.json \
      -m OpenSSH -i -s libssh
# start pshitt that will liste to port 2200
cd pshitt
./pshitt
# add a rules to redirect source IP from the set
iptables -A PREROUTING -t nat \
         -m set --match-set libssh src \
         -i eth0 -p tcp -m tcp --dport 22 \
         -j REDIRECT --to-ports 2200
```

Some results: most used passwords



Some results: les sused passwords



LESS USED PASSWORDS

Term	Count	Action
!!!111	1	
!$*lixiangyu610098	1	
!1@2#3	1	
!2#4	1	
!2#4%6	1	
!2#4%6&	1	
!@#$zzidcQWER10.3	1	
!@#19841010	1	
!Q2w#E4r%T6y	1	
!QAZ1qaz	1	
Other values	6127	

STAMUS NETWORKS

STAMUS NETWORKS

Conclusion

Don't fear to be sexy

- Sexy charts and interfaces are not only for finance guys thanks to Elasticsearch
- Suricata can boost the sex appeal of network monitoring

More information

- Suricata: `http://www.suricata-ids.org/`
- Netfilter: `http://www.netfilter.org/`
- Elasticsearch: `http://www.elasticsearch.org/`
- Suricata developers blogs: `http://planet.suricata-ids.org/`
- SELKS: `https://www.stamus-networks.com/open-source/#selks`
- My blog: `https://home.regit.org/`