Suricata

Victor Julien

OISF

July 7, 2014

About me

OISF

- ’founder’ and lead developer of Suricata IDS/IPS

Open Source

- Vuurmuur - firewall manager
- ModSecurity, libhtp, modsec2sguil, sguil, snort_inline

Contact

- @inliniac
- http://blog.inliniac.net/

About OISF

Open Information Security Foundation

- `http://www.openinfosecfoundation.org`
- Non-profit foundation organized to build a next generation IDS/IPS engine
- Funded by US Governement (DHS, Navy)
- Development of an Open Source IDS/IPS: Suricata

OISF Open Information Security Foundation

About OISF

- Consortium members
  - Platinium level: Lockheed Martin, nPulse Technologies
  - Gold level: Tilera, Altera, Endace, Emerging Threats
  - Bronze level: Everis, Myricom, Emulex
  - Technology partner: Napatech, Nvidia
- Developers
  - Victor Julien
  - Anoop Saldanha, Eric Leblond
  - various developers from consortium members
  - lots of community contributions
- Board
  - Matt Jonkmann
  - Richard Bejtlich, Dr. Jose Nazario, Ken Steele, Randy Caldejon, Luca Deri, Alexandre Dulaunoy

Goals

- Bring new technologies to IDS
- Give room to experimentation
- Performance
  - Multi-threading
  - Hardware acceleration
- Open source
- Support of Linux / *BSD / Mac OSX / Windows

Similar projects

Bro

- Different technology (capture oriented)
- Script based inspection and detection

Snort

- Equivalent
- Compatible
- Competing

Suricata vs Snort

Suricata

- Driven by a foundation, community
- Multi-threaded
- Native IPS
- Advanced functions (flowint, libHTP, lua)
- PF_RING support, CUDA support
- Modern and modular code
- Dynamic fast moving project

Snort

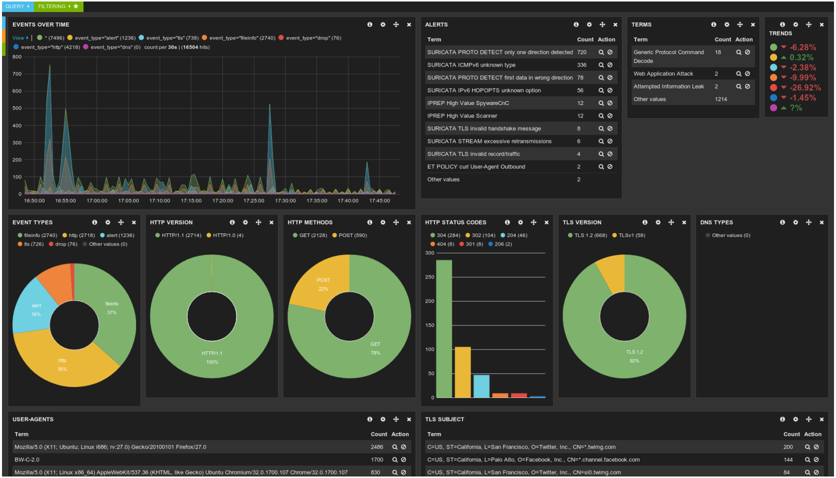
- Developed by Cisco/Sourcefire
- Multi-process
- IPS support
- SO ruleset (advanced logic + perf but closed)
- No hardware acceleration
- Old code

Features

- IPv6, IPS
- Multi-threaded
- Native hardware acceleration (PF_RING, Napatech, Endace, Tilera)
- IP lists, IP reputation, GeoIP
- Protocol detection
- Protocol Logging
- JSON output (logstash, splunk)
- Snort compatible rules
- Snort compatible output (unified2/barnyard2)
- Many more: http://suricata-ids.org/features/all-features/

Suricata with ELK

ELK: elastic search, logstash, kibana.


QUERY
FILTERING
EVENTS OVER TIME
View | ● * (7496) ● event_type="alert" (1236) ● event_type="tls" (738) ● event_type="fileinfo" (2740) ● event_type="drop" (76)
● event_type="http" (4218) ● event_type="dns" (0) count per 30s | (16504 hits)
800
700
600
500
400
300
200
100
0
16:50:00
16:55:00
17:00:00
17:05:00
17:10:00
17:15:00
17:20:00
17:25:00
17:30:00
17:35:00
17:40:00
17:45:00

ALERTS

Term	Count	Action
SURICATA PROTO DETECT only one direction detected	720	🔍 ⊘
SURICATA ICMPv6 unknown type	336	🔍 ⊘
SURICATA PROTO DETECT first data in wrong direction	78	🔍 ⊘
SURICATA IPv6 HOPOPTS unknown option	56	🔍 ⊘
IPREP High Value SpywareCnC	12	🔍 ⊘
IPREP High Value Scanner	12	🔍 ⊘
SURICATA TLS invalid handshake message	8	🔍 ⊘
SURICATA STREAM excessive retransmissions	6	🔍 ⊘
SURICATA TLS invalid record/traffic	4	🔍 ⊘
ET POLICY curl User-Agent Outbound	2	🔍 ⊘
Other values	2	

TERMS

Term	Count	Action
Generic Protocol Command Decode	18	🔍 ⊘
Web Application Attack	2	🔍 ⊘
Attempted Information Leak	2	🔍 ⊘
Other values	1214	

TRENDS

- ● ▼ -6.28%
- ● ▲ 0.32%
- ● ▼ -2.38%
- ● ▼ -9.99%
- ● ▼ -26.92%
- ● ▼ -1.45%
- ● ▲ ?%

USER-AGENTS

Term	Count	Action
Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:27.0) Gecko/20100101 Firefox/27.0	2486	🔍 ⊘
BW-C-2.0	1700	🔍 ⊘
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/32.0.1700.107 Chrome/32.0.1700.107	830	🔍 ⊘

TLS SUBJECT

Term	Count	Action
C=US, ST=California, L=San Francisco, O=Twitter, Inc., CN=*.twimg.com	200	🔍 ⊘
C=US, ST=California, L=Palo Alto, O=Facebook, Inc., CN=*.channel.facebook.com	144	🔍 ⊘
C=US, ST=California, L=San Francisco, O=Twitter, Inc., CN=si0.twimg.com	84	🔍 ⊘

IDS/IPS

Intrusion Detection System

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station. (source: Wikipedia)

Intrusion Prevention System

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. (source: Wikipedia)

IPS

- Positioned *inline*, as it needs to be able to block packets
- Can be done via routing or bridging
- Active response also possible, but less reliable
- Good fit for Netfilter

3 Suricata IPS modes

Netfilter

- Use libnetfilter_queue and NFQUEUE
- Verdict packet redirected by iptables rules

ipfw

- Uses divert socket
- Dedicated filtering rules must be added
- Supports FreeBSD and OS X

AF_PACKET

- Using Linux capture
- Transmit packets we allow, drop others
- Ethernet transparent mode

IPS Rule management

The transformation

- Make some rules start with *drop* instead of *alert*
- A selection must be made – not all rules suitable for dropping

Tool usage

- Rules are updated
- Tool are needed to make changes persistent
- Pulledpork: `http://code.google.com/p/pulledpork/`
- oinkmaster: `http://oinkmaster.sourceforge.net/`

Suricata in IPS mode

Using a Linux/Netfilter based IPS

- Use NFQUEUE to send decision to userspace
- All packets of a connection must be seen to Suricata
- The brutal way: iptables -A FORWARD -j NFQUEUE

Interaction with the firewall

- NFQUEUE is a terminating target
  - An ACCEPT decision will shortcut the whole ruleset
  - This is the only possible decision but DROP
- The previous method is thus incompatible with the existence of a ruleset.

NFLOG support

Why not IPS

- Sometimes mixing IDS and IPS is needed
- Blocking not acceptable and/or latency not acceptable
- False positive risk too high
- Detection and logging still required

Alternative

- We could use general IDS mode (-i eth0 / --af-packet=eth0)
- But that could lead to duplicate inspection when already using IPS
- Pcap capture method sees packets before iptables, so also packets that will be dropped
- Solution: NFLOG support

Suricata NFLOG support brought to you by:

Giusseppe Longo – @glongo01

NFLOG support 2

- NFLOG / libnetfilter_log sends packets to user space apps
- Like NFQUEUE, but non-terminating and no verdict
- Suricata support created by Giuseppe Longo
- http://blog.lupiae.org/capture-packets-from-nflog-in-suricata/

- Brute force: iptables -A FORWARD -j NFLOG

- Mixing with NFQUEUE is possible
- iptables -A FORWARD -p tcp -j NFQUEUE
- iptables -A FORWARD -p udp -j NFLOG
- Currently 2 Suricata instances needed

NFLOG support 3

IDS

- iptables -A FORWARD -j NFLOG --nflog-group 7
- suricata --nflog=7

IPS

- iptables -A FORWARD -j NFQUEUE --queue-num 10
- suricata -q 10

NFLOG support 4

Making things easy

- Create custom 'IDS' target
- iptables -N IDS
- iptables -A IDS -j NFLOG –nflog-group 7
- iptables -A IDS -j ACCEPT

Using the new target in rules

- iptables -A FORWARD -p tcp -j IDS
- suricata --nflog=7

NFLOG support 5

Future Work

- Benchmarking
- Suricata 'mixed mode' IDS and IPS: suricata -q 10 –nflog=7
- NIC offloading?