

Logging with Netfilter and ulogd2

Éric Leblond

Stamus Networks

June 23, 2015

- French
- Network security expert
- Free Software enthusiast
- NuFW project creator (Now ufw), 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

Packet logging

Syslog logging

- Flat packet logging
- One line per packet
- Use printk kernel facility

Syntax

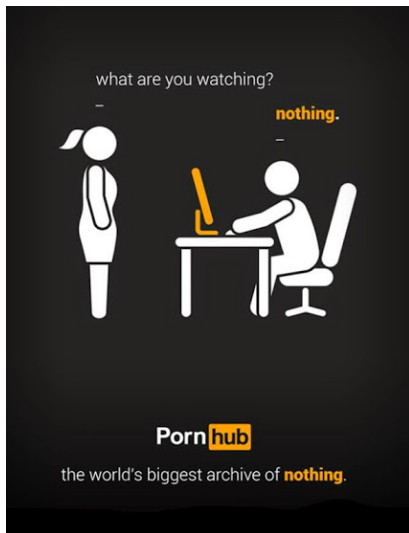
```
iptables -A INPUT -p tcp --dport 25 --syn \  
-j LOG --log-prefix "SMTP access "
```

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=91.121.73.151 LEN=60 TOS=0x00 PREC=0x00 \  
TTL=58 ID=35342 DF PROTO=TCP SPT=59261 DPT=113 WINDOW=5440 RES=0x00 SYN URGP=0
```

NETWORKING

Defensive security



Socket base messaging

- Netlink based communication
- Different groups
- Batching system
- IPv4 only

Syntax

```
iptables -A INPUT -p tcp --dport 25 --syn \  
-j ULOG --ulog-prefix "SMTP access" \  
--ulog-nlgroup 2 \  
--ulog-qthreshold 10
```

A logging daemon

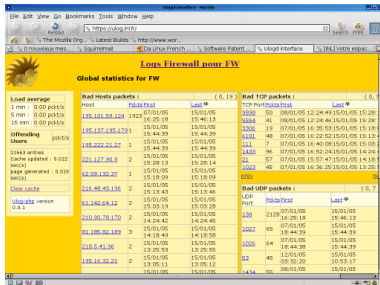
- Listen to event
- Store event in various formats
 - Flat file
 - Databases

Ulogd outputs

- LOGEMU
- OPRINT
- MySQL
- Postgresql
- sqlite3
- pcap

uologd: first interfaces

- Using SQL backend
- Providing a dashboard
- Nulog released 14 Apr 2000



The screenshot shows a web browser window displaying the uologd interface. The page title is "uologd interface" and the URL is "http://www.eric-leblond.com". The main content area is titled "Logs Firewall pour FW" and "Global statistics for FW". It features several tables of statistics, including "Load average", "Offloading", "Users", "Bad TCP packets", and "Bad UDP packets". The tables contain columns for "Host", "Packets", "Last", and "Count".

Load average	Host	Packets	Last	Count
1 min : 0.00 pkt/s	192.168.1.100	1922	07/01/05	15/01/05
5 min : 0.00 pkt/s		16 25 18	15/01/05	15/01/05
15 min : 0.00 pkt/s		15 01 05	15/01/05	15/01/05

Offloading	Host	Packets	Last	Count
Users	192.168.1.100	1	15/01/05	15/01/05
192.168.1.100	1	15/01/05	15/01/05	15/01/05
192.168.1.100	2	15/01/05	15/01/05	15/01/05

Bad TCP packets	Host	Packets	Last	Count	
2000	50	08/01/05	12 24 49	15/01/05	15 29
5554	41	08/01/05	12 24 46	15/01/05	15 29
1006	19	07/01/05	16 35 53	15/01/05	15 18

Bad UDP packets	Host	Packets	Last	Count	
6101	40	07/01/05	16 32 32	15/01/05	15 13
111	7	07/01/05	16 40 08	15/01/05	15 03
1452	98	07/01/05	16 52 34	15/01/05	14 24

2.6.14: the nfnetlink revolution

Nfnetlink

- First major evolution of Netfilter (Linux 2.6.14, 2005)
- Netfilter dedicated configuration and message passing mechanism

New interactions

- NFLOG: enhanced logging system
- NFQUEUE: improved userspace decision system
- NFCT: get information and update connection tracking entries

Based on Netlink

- datagram-oriented messaging system
- passing messages from kernel to user-space and vice-versa

Ulogd reloaded

- Interact with the post 2.6.14 libraries
- First release on 01 Feb 2006
- Multiple output and input through the use of stacks

Stack example

```
stack=log2:NFLOG,mark1:MARK,base1:BASE,ifil:IFINDEX,ip2bin1:IP2BIN,\  
    mac2str1:HWHDR,mysql1:MYSQL  
stack=log2:NFLOG,base1:BASE,ifil:IFINDEX,ip2str1:IP2STR,\  
    mac2str1:HWHDR,pgsql1:PGSQL
```

Nothing really new

- One ulogd2 can handle multiple logging input
- Multiple output is also supported

But improved databases

- Magical schema discovery
- Better schema
- Insertion via SQL procedure
 - It is possible to create custom logging in SQL
 - No need to know C

ulogd2: connection logging

Interests

- Log volume of exchange data
- Log NAT transformation

Ulogd2 support

- File and database output

```
stack=ct2:NFCT,ip2str1:IP2STR,pgsql2:PGSQL
```

More info <https://home.regit.org/2014/02/logging-connection-tracking-event-with-ulozd/>

nfacct

- Efficient accounting system
- Appeared in 2012

In ulogd

- Dump nfacct counter at regular interval
- Realize storage
 - XML
 - Postgresql
 - Graphite

Graphite

- Scalable Realtime Graphing
- Based on rrdtools
- Allow to combine data
- <http://graphite.wikidot.com/start>

Alternate

- Frontend: Grafana
- Backend: Influxdb

Ulogd2 configuration

```
stack=acct1:NFACCT,\
      graphite1:GRAPHITE

[acct1]
pollinterval = 2

[graphite1]
host="127.0.0.1"
port="2003"
```

ulogd2: graphite



JSON output

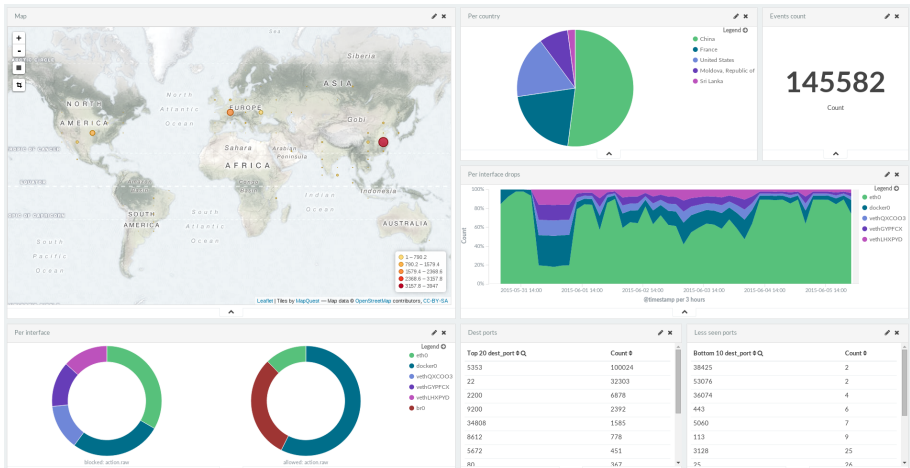
JSON format

- Formatted message
- Schema less
- Easy to use in code and tools
- Integration with Splunk or Elasticsearch

JSON plugin

- Use ulogd key, value system
- Translation to text of key is enough
- Usable for all input plugins

Demo: Ulogd + Kibana



Conclusion

Ulogd2 brings complete logging to Netfilter

- Packets logging
- Connection tracking logging
- Accounting

More information

- **Netfilter:** <http://www.netfilter.org/>
- **My blog:** <https://home.regit.org/>
- **Stamus Networks:** <https://www.stamus-networks.com/>