What is Haka

Haka is an open source security oriented language which allows to describe protocols and apply security policies on (live) captured traffic.

The scope of Haka language is twofold. First of all, it allows to write **security rules** in order to filter/alter/drop unwanted packets and log and report malicious activities. Second, Haka features a **grammar** enabling to specify network protocols and their underlying **state machine**.

The overall goal of Haka is to abstract low-level stuff like memory management and packet reassembly to non developer experts and to provide an easy way to analyze quickly new network protocols.

The Haka team is proud to announce the release of **Hakabana (http://www.haka-security.org/hakabana.html)**. A tool to visualize network traffic going throught **Haka** in real-time using **Kibana** and **Elasticsearch**.

Packet filtering policy improved

Define your own security rules to alter/drop/inject packets based on combination of protocol fields (ip, tcp, udp, icmp, dns and http).

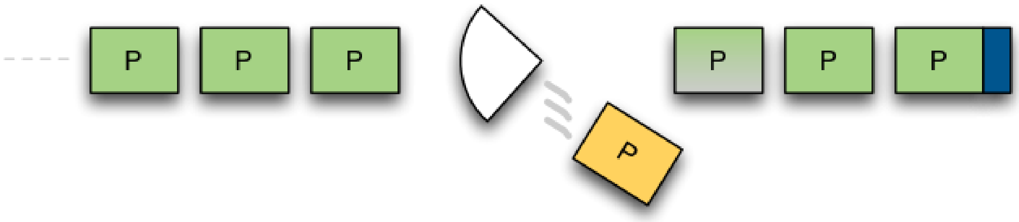
```
local ipv4 = require('protocol/ipv4')

haka.rule{
    hook = ipv4.events.receive_packet,
    eval = function (self, pkt)
        if pkt.src ~= ipv4.addr("127.0.0.1") then
            pkt:drop()
        end
    end
}
```

Packet capture

Use various sources of traffic for packet filtering, including:

- pcap file
- pcap live traffic
- netfilter queue iptable rules



Protocol grammar new

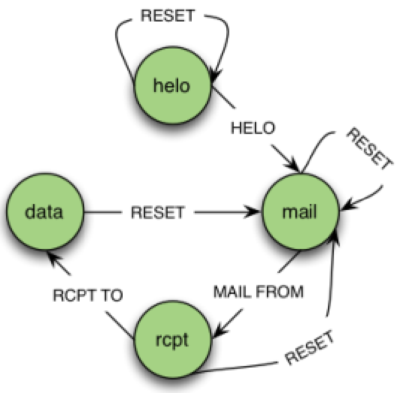
Protocol parsing is simple, describe the messages in Haka and let the engine do the parsing.

```
haka.grammar.new("icmp", function ()
    packet = record{
        field('type',     number(8)),
        field('code',     number(8)),
        field('checksum', number(16)),
        field('payload',  bytes())
    }

    export(packet)
end)
```

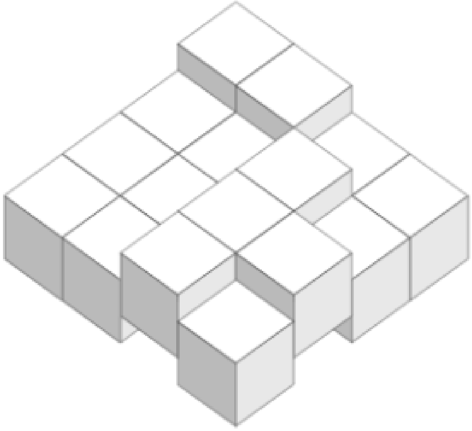
Protocol state machine new

Quickly and easily describe protocol state machines directly in Haka. Describe your states and transitions and let the internal Haka engine follow them.



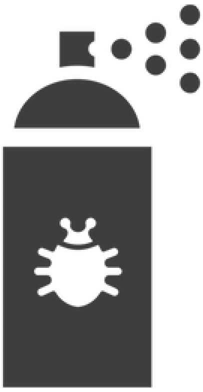
Modular, extensible

Haka has a modular design which allows easy customisation. The internal and external APIs are well documented and allow anyone to easily add new protocols, capture methods, logging sinks...



Integrated debugger

Back-trace, insert breakpoints and inspect Lua code. Haka is endowed with a gdb-like debugger which is helpful to detect errors in Lua security rules.



Going further !

Full workshop new

A full workshop is available for you to dig into Haka. Check out our **bootable live iso! (http://www.haka-security.org/download/haka.html)**

Hakabana new

Visualize network traffic going throught **Haka** in real-time using **Kibana** and **Elasticsearch**. Check out **Hakabana (http://www.haka-security.org/hakabana.html)**.

(http://www.haka-security.org/hakabana.html)

What's next...

Next release will focus on improving the Haka performances and simplify even more security rules and protocol description.