Status on the project and some proposals
What's this?

- New version of old ulogd

- Able to use libnfnetlink stuff as entry:
  - conntrack
  - log

- Modular:
  - Uses filter flow
  - stack=ct1:NFCT,print1:PRINTFLOW,emu1:LOGE
Status

- **Bad points**
  - Last beta release in 2005
  - Some important bugfix since then
  - Not usable because of lack of documentation

- **Good points**
  - Really modular
  - Able to work with nfnetlink_conntrack or nfnetlink_log
Ulogd like feature

- Ulogd2 is able to log to SQL database
  - mysql support
  - postgresql support
  - ...

- SQL design issue
  - All is stored in a single table
  - Simple
  - Not modular (pwsniff feature ;)

Improving SQL schema?

• Switching to an index oriented schema:
  - Storing separately components
  - Limit database size
  - Avoid the NULL value approach

• Will achieve modularity
Discussions

- Is this kind of evolution admissible to upstream?
- Who could join the project?