nftables error reporting

NFWS 2017 - Faro, Portugal

Pablo Neira Ayuso
<pablo@netfilter.org>

Sparse grain error reporting

- What is wrong with?
  - nft add rule x y counter
    <cmdline>:1:1-21: Error: Could not process rule: No such file or directory
    add rule x y counter
    ^^^^^^^^^^^^^^^^^^^^
- Reason?
  - Table does not exist
  - Chain does not exist
  - Kernel doesn't come with counter support?

Netlink extended error reporting

- Added during NetDev 2.1 in Montreal
- Idea:
  - New netlink socket option
  - Kernel sends us an extended netlink ACK
  - Includes offset to attribute that has caused the problem

Error report scenarios

- Start with something simple...
  - Missing object
    - Table/Chain/Set/Object does not exist
  - Statement is not supported
  - What else?

Nftables implementation

- Store struct location (loc) in struct nftnl_xyz
  - nftnl_table_set_set(nlt, NFTNL_TABLE_NAME, “test”, &loc);
- libnftnl build func maps attribute offset ↔ loc
- On error, fetch attribute offset to lookup for loc
- Needs...
  - libmnl extension to return attribute offset
  - More structure location for handles