Netfilter userspace updates (since June 2015)

Pablo Neira Ayuso
<pablo@netfilter.org>

A bit of stats

- Iptables: 123 unique authors
  - Shivani: 48 commits
  - Pablo: 15 commits
  - Laura: 12 commits
  - Roberto: 12 commits
  - Florian: 4 commits
- Release of 1.6.0 (first version including iptables-compat)

Iptables

- -m socket –restore-skmark (Qualcomm)
- missing icmpv6 dest-unreach (Andreas Herz)
- Zone direction support (Daniel Borkmann)
- Cgroup2 support (Tejun Heo)
- Add translation infrastructure
  - … and start providing translations
- NFQUEUE target parser fixes (Shivani)
- NETMAP listing fix (Florian Westphal)
- Missing warn on DROP from IPv6 nat table

A bit of stats (2)

- nftables: 12 unique authors
  - Pablo: 117
  - Florian: 58
  - Arturo: 30
- Two releases:
  - 0.5 in September 16th, 2015
  - 0.6 in June 2th, 2016

nftables

- Many fixes
- Lots of new unit tests
- New shell test infrastructure (Arturo Borrero)
- Support for incremental updates
  - Rework netlink cache infrastructure
- Support for VLAN header matching (Florian & Pablo)
- Non-8-bit bound fields support (Florian & Pablo)
- Limit per-byte & bursts, dup, fwd
- Ruleset listing filtering enhacements

nftables (2)

- dynamic map fix: failing at evaluation
- Rule replacement (Carlos Falgueras)
- Interface name prefix matching, eg. eth*
- filtering on L2 header in inet family (Florian)
- Payload statement (Patrick)
- ct directional keys (Florian)
- ct counter comparison (Florian)

nftables (3)

- add icmpv6 types (Shivani)
- enforce ip6 proto with exthdr expression (Florian)
- allow 'snat' and 'dnat' keywords from the right-hand side
- Add router advertisement and solicitation icmp types (Laura)
- User data for sets (Carlos Falgueras)
- nft monitor trace (Patrick)
- Flow tables (Patrick)
- Interval/range elements with dynamic sets (Pablo)

A bit of stats (3)

- libnftnl: 8 unique authors
  - 22 Pablo Neira Ayuso
  - 11 Carlos Falgueras García
  - 4 Florian Westphal
- Releases:
  - 1.0.5 in September, 16th 2015
  - 1.0.6 in May, 30th 2016

libnftnl

- Limit expression per-byte & burst
- Payload expression for mangling and trace
- Dup, fwd expression
- Ct counter support
- TLV for userdata
- Larger set names (up to 32 bytes)
- Inverted lookups for sets

A bit of stats (4)

- conntrack-tools: 9 unique authors
  - 15 Asbjørn Sloth Tønnesen
  - 14 Pablo Neira Ayuso
  - 10 Mart Frauenlob
  - 7 Arturo Borrero
  - 3 Szilárd Pfeiffer
- Releases:
  - conntrack-tools 1.4.3

Conntrack-tools

- IPv6 NAT support for state-sync (Arturo Borrero)
- Manpages fixes (Mart Frauenlob)
- CIDR-based list filtering (A.S.Tønnesen)
- nfct syntax updates
- State-sync network message sanitization after RH security reports
- Fix expectation creation (Szilárd Pfeiffer)

More thoughts

- Deprecate libnfnetlink and use libmnl in existing codebase?
- Missing unit tests for libraries and utilities.
- Doxygen for libnftnl.