A look at netfilter's bugzilla

Pablo Neira Ayuso
<pablo@netfilter.org>

nftables

- Broken interface prefix from sets (1059)
  - Working already from plain rules
  - Revisit interval logic in userspace
- Missing logging options (921)
  - IP & TCP options, uid
- Use of variable declaration from variable definition (1042)
- Not possible to invert a set (923)
  - Arturo already submitted patches

nftables (2)

- Problems with ranges and names (1046)
  - Eg. mh type 1-2

    mh type home-test-init-careof-test-init
- Missing icmp types? (925, 926)
- SCTP chunk types (929) and DCCP options (930) and TCP options (1058)
  - Add this to exthdr expression
- Mangling of TCP options (1058)
- Attach ct template (942) and NOTRACK is not supported (1065)

nftables (3)

- ICMP from inet family (1073)
  - Easy to fix in loose way matching ICMPV6_PROTO
  - Needs extra dependency to enforce Ipv6
    - Meta proto
- mld-listener-query not honored (998)
- Use of keywords as value from sk uid (1037)
- Include statement search for file in /etc (1040)
- Add set using ipv4_address datatype to Ipv6 table (895)

nftables (4)

- Set protocol context from sets (1027)
  - eg. ip protocol { udp, tcp } snat 1.2.3.4:1024-2048
- Broken icmp code matching (949)
- SYNPROXY (1054)
- Meta priority broken (953)

iptables

- iptables-save output depends on module loading order (580)
- Per rule counter reset (912)
  - Tighten syntax to reject this upfront since this is not supported
- Update manpage to indicate that iptables-save only displays module loaded tables (960)
  - User confused, should be easy to document behaviour
- Better error reporting (944)
  - Provide this from nftables

Iptables (2)

- Iptables-save to file as option, instead of using stdout redirection (905)
- Policy match and Ipv6 addresses (892)
- Better documentation for TRACE target (1076)
- Extend REJECT (696), crazy?
  - User wants to indicate what direction to reset: original, reply, both.
- Compilation breaks with --enable-static and missing libnetfilter_conntrack (1024)
  - I think this is already fixed, confirm this.

Iptables (3)

- Multitarget rules in iptables (657): nft already does
- Iptables -p all problems (1015), means match any, but -p 0 is a valid protocol
- Icmp types ranges (630)
- Use getaddrinfo instead gethostbyaddr (989)
  - Already patch in patchwork, will review and apply
- Unexpected behaviour in recent (961)
- Several conntrack match (875), error report if -m state INVALID,NEW (874) and (873)
- Problems with iptables and x32 ABI and compat (1025)

Patchwork

- Reports on H.323 helper problems
  - This code needs wider review and some care
- Problem with checksumming in IPv6 and NAT
  - Patch submitted, feedback from Tom Herbert
- Include directories in nftables
  - glob() to allow file patterns
  - Loops via for
- Clang problems with our EXPORT_SYMBOL declaration
  - #define __visible   __attribute__((visibility("default")))
  - #define EXPORT_SYMBOL(x) typeof(x) (x) __visible
- Netns exit path and module removal race
  - Netns exit path runs from workqueue => wait for completion