netsniff-ng toolkit: Swiss army knife for network development and debugging

(Lightning Talk)

Daniel Borkmann
<dborkman@redhat.com>
http://netsniff-ng.org

Netfilter Workshop, Copenhagen, March 9, 2013

Netsniff-NG Toolkit

- Useful networking toolkit for daily kernel plumbing, security auditing, system monitoring or administration
- Set of minimal tools: **netsniff-ng**, **trafgen**, **astraceroute**, **curvetun**, **ifpps**, **bpfc**, **flowtop**, **mausezahn**
- Core developers: Daniel Borkmann[1], Tobias Klauser[2], Markus Amend, Emmanuel Roullit, Christoph Jäger, Jon Schipp (documentation)
- `git clone git://github.com/borkmann/netsniff-ng.git`
- Project since 2009, started just for fun; GNU GPL, version 2.0

[1] Project Maintainer

Netsniff-NG Toolkit

- Useful networking toolkit for daily kernel plumbing, security auditing, system monitoring or administration
- Set of minimal tools: **netsniff-ng**, **trafgen**, **astraceroute**, **curvetun**, **ifpps**, **bpfc**, **flowtop**, **mausezahn**
- Core developers: Daniel Borkmann[1], Tobias Klauser[2], Markus Amend, Emmanuel Roullit, Christoph Jäger, Jon Schipp (documentation)
- `git clone git://github.com/borkmann/netsniff-ng.git`
- Project since 2009, started just for fun; GNU GPL, version 2.0

[1] Project Maintainer

bpfc

- Minimal, low-level BPF “compiler” (converts BPF “asm” to opcodes)
- Understands internal kernel extensions
- Example use cases:
  - Config tool for recently published `xt_bpf` from Google
  - Filters that libpcap/tcpdump might not support
  - Writing BPF JIT proof of concept exploits[2]
- Short demo

[2] `http://carnivore.it/2011/12/27/linux_3.0_bpf_jit_x86_64_exploit`

trafgen

- Low-level traffic generator based on `PF_PACKET`'s `TX_RING`
- Multi-threaded, flexible config language, can be used with `tc(8)`
- Example use cases:
  - Various kinds of stress-testing for behavioral analysis[3]
  - Smoke/fuzz testing firmware, stacks or applications
  - Support for 802.11 injection
- Short demo

[3] `http://lists.openwall.net/netdev/2013/01/29/44`

ifpps

- Top-like networking and system statistics (pps, IRQs, SoftIRQs, etc.)
- Optional Gnuplot output mode
- Short demo

Thanks! Questions?

- Go hack on it! ;-)
  - `git clone git://github.com/borkmann/netsniff-ng.git`
- Web: `http://netsniff-ng.org`