top-like connection tracking with flowtop

(Lightning Talk)

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

Netfilter Workshop, Copenhagen, March 9, 2013

Motivation

- Useful to have a quick overview of current connections
  - If you access website X, what other connections are being opened in the background that I'm not aware of?
  - What connections are active that pass ones router?
  - I have this proprietary binary Y, where does it connect to?
  - To which countries am I sending my data?
  - Are there any suspicious background connections on my machine?
  - How many connections has binary Z currently active?

flowtop

- Built on top of `libnetfilter_conntrack` library
- Top-like ncurses frontend for displaying flows/sessions
- What it currently displays per flow, if available:
  - Application name and PID
  - Used protocols (IPv4, IPv6, TCP, UDP, SCTP, ICMP, ...)
  - Transport protocol state machine information, e.g. for TCP
  - Used flow port/service heuristic
  - Reverse DNS for source and destination, ports
  - Geo-location information (country, city)
- Short demo

Thanks! Questions?

- flowtop is part of the netsniff-ng toolkit
- Go hack on it! ;-)
  - `git clone git://github.com/borkmann/netsniff-ng.git`
- Web: `http://netsniff-ng.org`

Project Proposals

- Include `libnetfilter_conntrack` byte, packet counter
- Add a filtering system
  - glibc's regex for application names, geo information or on DNS names
  - Filtering based on PID, ports
- Figure out a way to display information more nicely
- Also allow to dump information, or non-ncurses output