Sniffer – libpcap

František Uchytil

České vysoké učení technické v Praze, 2008

Obsah

Co je pcap?

- Je to knihovna, která nám usnadňuje práci při *odchytávání paketů*.
- Její síla tkví nejen v rychlosti naprogramování, ale hlavně v *komplexní sadě filtrovacích pravidel*.

Jak se s tím pracuje?

1. Určíme *zařízení*, na kterém budeme odchytávat pakety (`eth0, xl1`, ...).
2. Nastavíme pcap, aby *poslouchal* na tomto zařízení. Je možno poslouchat z více zařízení současně, nebo si pakety brát ze souboru.
3. Pokud nás zajímá jen určitý tok dat (IP, ETHERNET, TCP, ...), tak vytvoříme sadu *pravidel*, překompilujeme je a nastavíme.
4. Nyní můžeme vstoupit do smyčky a *parzovat* pakety, které nám pcap naservíruje.
5. Nakonec je slušnost vše vrátit do původní podoby (*uzavření* zařízení, ...)

Co bylo mým úkolem?

- Sledovat průtok dat v jednotlivých sítích (např.: 1.2.3.4/5).
- Rozpoznat protokoly, přes které se komunikuje. Omezil jsem se na TCP, UDP, ICMP a IP.
- Program může fungovat jako filtr (tzn. čtení z `stdin` a zápis na `stdout`).
- Je napsán tak, aby se dal jednoduše rozšířit.

Zdroje

Web

1. http://www.tcpdump.org/
2. http://www.wikipedia.org/