Flex

Zadanie polega na stworzeniu **skanera do analizy logów w formacie tcpdump** (tcpdump manual).

Skaner ma wypisywać informację o tym z jakimi adresami (i na jakie porty) łączył się użytkownik. Pod uwagę proszę wziąć protokóły tcp i icmp. Adres użytkownika (w przykladzie FARM1) powinien być podawany jako parametr wywołania skanera.

Przykładowo dla wejścia:

```
11:10:20.208054 IP FARM1.1333 > 216.239.59.104.80: S 1971158991:1971158991(0) wi...
11:10:20.267067 IP 216.239.59.104.80 > FARM1.1333: S 1948826897:1948826897(0) ac...
11:10:48.133405 IP FARM1.1334 > luke.icsr.agh.edu.pl.22: S 605740831:605740831(0...
11:10:48.133643 IP luke.icsr.agh.edu.pl.22 > FARM1.1334: S 1596621236:1596621236...
11:10:48.133958 IP FARM1.1334 > luke.icsr.agh.edu.pl.22: . ack 1 win 65535
11:10:48.137980 IP luke.icsr.agh.edu.pl.22 > FARM1.1334: P 1:24(23) ack 1 win 32...
11:10:48.321969 IP luke.icsr.agh.edu.pl.22 > FARM1.1334: P 300:312(12) ack 184 w...
11:10:48.432329 IP FARM1.1334 > luke.icsr.agh.edu.pl.22: . ack 312 win 65224
11:10:52.790004 IP FARM1.1335 > arax.uci.agh.edu.pl.80: S 3711582108:3711582108(...
11:10:52.790715 IP arax.uci.agh.edu.pl.80 > FARM1.1335: S 2071915938:2071915938(...
11:11:09.927425 IP FARM1 > f1virt.onet.pl: icmp 40: echo request seq 12544
11:11:09.929286 IP f1virt.onet.pl > FARM1: icmp 40: echo reply seq 12544
```

na wyjściu powinno pojawić się:

```
216.239.59.104 tcp 80
luke.icsr.agh.edu.pl tcp 22
arax.uci.agh.edu.pl tcp 80
f1virt.onet.pl icmp
```

Linie w nieprawidłowym formacie powinny być pominięte.

W zadaniu należy wykorzystać generator skanerów flex (flex manual)

Przyładowy log tcpdump: example-log

Inne materiały

monitoring with tcpdump
tools: tcpdump
Lex - A Lexical Analyzer Generator, M. E. Lesk