Analyzátor sieťovej komunikácie

Patrik Siget

Zadanie:

Navrhnite a implementujte analyzátor Ethernet siete, ktorý analyzuje komunikácie v sieti zaznamenané v .pcap súbore.

Koncepcia fungovania riešenia:
Program načíta súbor .pcap a pokiaľ nie je špecifikovaný filter, vypíše celý súbor analyzovaný len na 2. Vrstve, ako bolo názorne ukázané v zadaní v bode 1. Pokiaľ je filter daný, analyzuje sa rámec, potom packet a tam sa nasledujúce vnorenie rozhodne podľa protokolu. Celý výpis rámca sa postupne zapisuje do dočasného súboru a nakoniec podľa filtra sa rozhodne, či sa má daný rámec vypísať.

Externé súbory na určenie protokolov a portov:
Súbory sú uložené v .ini súboroch. Príklad:

```
[icmp]
Echo_reply=0
Destination_Unreachable=3
Source_Quench=4
Redirect=5
Echo=8
Router_Advertisement=9
Router_Selection=10
Time_Exceeded=11
Parameter_Problem=12
Timestamp=13
Timestamp_Reply=14
Information_Request=15
Informatio_Reply=16
Address_Mask_Request=17
Address_Mask_Reply=18
Traceroute=30
```

Tento konkrétny súbor sa používa na výpis ICMP kódu. Program súbor načíta a podľa hodnoty vráti retazec.

UI:

Spustenie programu:

./analyze

- Vypíše nápovedu ako používať program.

./analyze --file “cesta do .pcap súboru”

- Vypíše celý súbor s analýzou 2. Vrstvy (bod 1)

./analyze --file “cesta” -f [filter]

- Vypíše len komunikáciu pod daným protokolom.

Možnosti:

- Tcp, udp, http, https, telnet, ssh, ftp-control, ftp-data, tftp, icmp

Voľba implementačného prostredia:

Program je napísaný v jazyku C. Kompilátor gcc 7.3.0 na operačnom systéme Ubuntu. Textový editor používam VScode.