Projekt do predmetu Síťové aplikace a správa sítí

Generování NetFlow dat ze zachycené síťové komunikace

Lukáš Neupauer xneupaa01

2022

Úvod

Účelom projektu je vytvoriť terminalovu aplikáciu, ktorá bude čitat zachytenú komunikáciu z pcap súboru a generovať z nej zachytené toky a odosielať ich na zachytávač.

Implementacia

Projekt je implementovaný v jazyku C, ku ktorému je aj príslušný makefile. Program podporuje netflow v5 štandart. Program podporuje iba štandart IPv4 ale nie IPv6.

Štruktúry a premenné

Toky sú zachytávané a ukladané v štruktúre NF5_header pre hlavičku toku a NF5_flow pre samotny tok. Tieto štruktúry sú spojené dokopy v štruktúre complete_flow. To znamená, že na jeden odoslaný tok pripadá jedna hlavička. Následne sú tieto štruktúry uložené v obojsmerne viazanom zozname pre efektívnu manipuláciu s nimi.

Všetky dôležité premenné sú v programe ako globálne premenné pre jednoduchšiu manipuláciu s nimi.

Zachýtávanie toku

Program pri po spustení a spracovaní argumentov sa snaží pripojiť na server pomocou UDP spojenia. Pri neúspešnom pripojení sa program ukončí s chybovým hlásením a vrati hodnotu 1. Pakety sú čítané v hlavnej smyčke programu, pokiaľ sa nenačítajú všetky pakety.

Z načítaného paketu sa najprv vezme časová značka a kontrolujú sa časové limity rozpracovaných tokov.To prebieha pomocou funkcie timer(). Následne sa inicializuje ethernetová a ip hlavička a zisti sa protokol funkciou initialize_values(). Ak sa nejedná o ip paket, tak sa paket zahodí. Ak je paket inaho protokolu ako TCP, UDP alebo ICMP tak za tatiež zahodí. Následne sa načíta hlavička protokolu a volá sa funkcia new_packet().

Táto funkcia zisti či paket patrí do už vytvoreného toku a priradí ho k nemu, alebo vytvorí nový tok v zozname. Následne sa zisťuje, či nie je dosiahnutý maximálny počet rozpracovaných tokov a ak áno, tak sa odošle najstarší v tomto prípade prvý v zozname, keďže predpokladáme, že pakety boli zachytené postupne priebehom času od najstaršieho. Pakety sa odosielajú pomocou funkcie export(). Pri neúspešnom odoslaní sa vypíše upozornenie, ale program beží ďalej.

Funkcie

void parse_arguments()

Spracuje argumenty z príkazového riadku. A nastavý zakladne nastavenie programu a časovače, zdrojový súbor či maximálny počet tokov.

void initialize_values()

Nastavuje ethernotovú a ip hlavičku a zisťuje protokol.

void new_packet()

Volá sa nad každým načítaným validným paketom. Priraduje pakety do tokov a nastavuje v nich hodnoty, ktoré dostane ako argumenty.

void export()

Odosiela tok, ktorý dostane ako argument na zberač.

void timer()

Kontroluje časovače na základe času ktorý dostane ako argument.