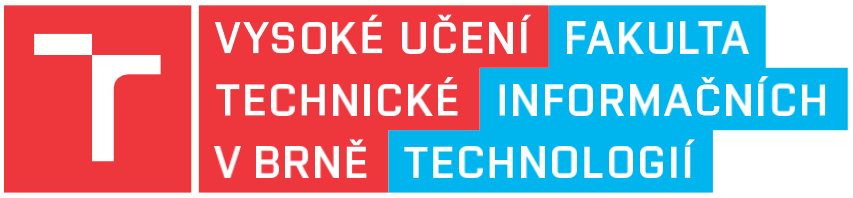

Síťové aplikace a správa sítí

Generování NetFlow dat ze zachycené síťové komunikace

14. listopad 2022 Adrián Matušík (xmatus35)

OBSAH

1 Úvod

Ciel'om projektu bolo implementovat' NetFlow exportér, ktorý zo zachytených sieťových dát vo formáte pcap vytvorí záznamy NetFlow, ktoré odošle na kolektor.

2 Implementácia

Program je navrhnutý v jazyku C++.

Najkôr kontroluje vstupné argumenty, ktoré sú všetky voliteľné, ale každý argument ma svoju predvolenú hodnotu.

Pokračuje čítaním z stdin alebo .pcap súboru, odkiaľ získa všetky potrebné informácie o protokoloch(ICMP, TCP, UDP).

Zo získaných dát sa vytvára kľúč, ktorý sa skladá z pätice (source IP, destination IP, source port, destination port, protocol). Pakety, ktoré majú túto päticu dát rovnakú sa agregujú do jedného toku.

Ďalej sa vkladajú jednotlivé pakety. Ak v mape neexistuje paket s rovnakou päticou, tak sa vytvára nový tok, do ktorého sa ukladá aktuálny paket, v prípade že paket s rovnakou päticou existuje, tak sa kontroluje či v poslednom pakete daného toku nie je príznak FIN príznak RST, alebo prekročený active alebo inactive timer. A pokiaľ paket s rovnakou päticou existuje ale neprekročilo žiadny z daných časov, ani neobsahuje žiadny z daných príznakov, tak sa aktualizujú určité hodnoty daného flowu.

V prípade že sa poruší podmienka, tak sa daný tok vloží do druhej "expiračnej" mapy v ktorej čaká dokým pride tridsiaty paket aby sa exportovali. Pokiaľ bude paketov menej ako 30 tak sa exportujú na konci behu program.

Po zaslaní toku do epiračnej mapy sa znovu vytvára nový tok pre aktuálny paket.

Na koniec programu sú všetky toky poslané na kolektor.

3 Použitie

Program musí podporovať nasledujúcu syntax pre spustenie:

./flow [-f <file>] [-c <netflow_collector>[:<port>]] [-a <active_timer>] [-i <inactive_timer>] [-m <count>]

-f <file> meno analyzovaného súboru alebo STDIN,

-c <neflow_collector:port> IP adresa, alebo hostname NetFlow kolektoru. voliteľne aj UDP port (127.0.0.1:2055, pokiaľ neni špecifikované),

-a <active_timer> - interval v sekundách, po ktorom sa exportujú aktívne záznamy na kolektor (60, pokiaľ neni špecifikované),

-i <seconds> - interval v sekundách, po jeho vypršaní sa exportujú neaktívne záznamy na kolektor (10, pokiaľ neni špecifikované),

-m <count> - veľkosť flow-cache. Pri dosiahnutí max. veľkosti dôjde k exportu najstaršieho záznamu v cachi na kolektor (1024, pokiaľ neni špecifikované).

Všetky parametre sú brané ako volitelné. Pokiaľ niektorý z parametrov neni uvedený, použije sa miesto neho predvolená hodnota.

Příklad použití:

./flow -f input.pcap -c 192.168.0.1:2055

4 Použitá literatúra

https://en.wikipedia.org/wiki/NetFlow
https://www.cisco.com/c/en/us/td/docs/net_mgmt/netflow_collection_engine/3-6/user/guide/format.html#wp1003394
https://en.cppreference.com/w/cpp/utility/tuple
https://en.cppreference.com/w/cpp/container/map
https://www.ibm.com/docs/en/zos/2.3.0?topic=functions-sendto-send-data-socket
https://linux.die.net/man/3/ntohl
https://moodle.vut.cz/course/view.php?id=231021
https://www.tcpdump.org/pcap.html