VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULT INFORMAČNÍCH TECHNOLOGIÍ

Síťové aplikace a správa sítí – projekt

Generování NetFlow dat ze zachycené síťové komunikace

14. listopadu 2022 Jakub Křinánek

Obsah

1 Úvod

V rámci tohoto projektu bylo za úkol navrhnout a implementovat NetFlow exportér, který ze zachycených síťových dat ve formátu pcap vytvoří záznamy NetFlow, které odešle na kolektor. Projekt byl implementován v `C++`.

2 Spouštění programu

Za pomocí souboru `Makefile` a použití programu `make` se program přeloží:

```
$ make
```

Poté je možné program spustit:

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

Všechny parametry jsou brány jako volitelné. Pokud některý z parametrů není uveden, použije se místo něj výchozí hodnota.

Popis parametrů:

- -f <file> - udává, z kterého souboru se budou packety načítat
- -c <netflow_collector:port> - IP adresa, nebo hostname NetFlow kolektoru. Volitelně i UDP port.
- -a <active_timer> - interval v sekundách, po kterém se exportují aktivní záznamy na kolektor
- -i <inactive_timer> - interval v sekundách, po jehož vypršení se exportují neaktivní záznamy na kolektor
- -m <count> - velikost flow-cache. Při dosažení max. velikosti dojde k exportu nejstaršího záznamu v cache na kolektor

Výchozí hodnoty:

- -f <file> - STDIN
- -c <netflow_collector:port> - 127.0.0.1:2055
- -a <active_timer> - 60
- -i <inactive_timer> - 10
- -m <count> - 1024

3 Knihovny

Knihovny použité v projektu jsou:

- <getopt.h> - zpracování argumentů
- <pcap.h> - příjmání packetů
- práce s packety
  <netinet/ether.h>
  <netinet/ip.h>
  <netinet/udp.h>
  <netinet/tcp.h>
  <netinet/ip_icmp.h>

4 Implementace

Na začátku programu se vytvoří objekt třídy `prog_args` a přes metody této třídy se vyhodnotí argumenty. Následně začíná čtení packetů, kdy se začnout tvořit objekty třídy `packet`. Tento packet následně zpracuje. Po zpracování předán exportéru. Po zpracování packetu exportérem se přečte další packet ze souboru a takto program pokračuje dokud nepřečte všechny packety.

Jako inspirace pro implementaci byl využit studentský stream[3] a studentský guide[2].

4.1 Fungování exportéru

Vždy když exportér dostane packtet porovnává jeho vlastnosti se všemy současnými flows v cache.

Vlastnosti flow, které se musí shodovat, aby packet patřil do flow:

- src_id - zdrojová ip adresa
- dst_id - cílová ip adresa
- src_port - zdrojový port
- dst_port - cílový port
- prot - protokol
- tos - type of service

Pokud se právě zpracovávaný packet zhoduje s nějakým flow v cache, je tento flow upraven. To znamená inkrementace počtu packetů, změna posledního času, přičtena velikost packetu a přidání TCP flags (v případě TCP packetu).

Pokud se s žádným flow neshoduje, je vytvořen nový flow a je umístěn do cache.

Poté probíhá kontrola active a inactive časů, kdy se prochází všechny flows v cache a pokud nějaký čas z flow vyprší, je tento flow exportován. Exportování probíhá posíláním UDP packetu na kolektor. Formát obsahu podle[1].

4.2 Omezení

Program plně funguje pro IPv4 a to pouze pro TCP, ICMP a UDP packety. V ostatních případech není zaručena správnost chování programu.

5 Testování

Pro testování byly použity programy nfdump, nfcapd a Wireshark.

Použité zdroje

[1] NetFlow Export Datagram Format. [online], rev. 14. září 2007, [vid. 2022-10-14].
URL https://www.cisco.com/c/en/us/td/docs/net_mgmt/netflow_collection_engine/3-6/user/guide/format.html#wp1003394

[2] Kendik: ISA - NetFlow Projekt Guide. [online], rev. 2. říjen 2022, [vid. 2022-10-09].
URL https://arc.net/e/2481E66A-A59E-4757-81B0-18AC7DDADF28

[3] Kuzník: ISA - netflow stream. [online], rev. 2. říjen 2022, [vid. 2022-10-11].
URL https://drive.google.com/file/d/16aPBd4lym5PgQlfPFgdq6POYW0Fw-qut/view?usp=sharing