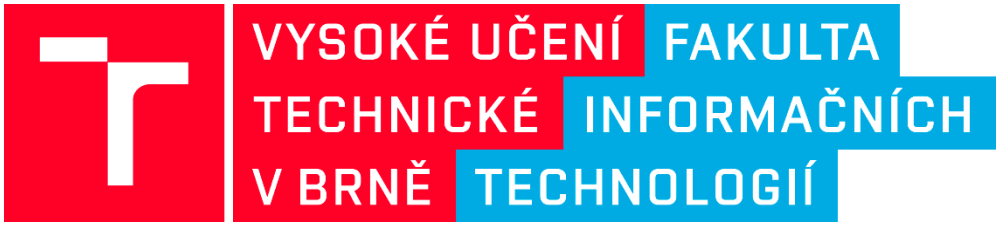
Vysoké učení technické v Brně

Fakulta informačních technologií



ISA

Síťové aplikace a správa sítí

2022/2023

Technická správa

Generování NetFlow dat ze zachycené síťové komunikace

Vedúci:

Ing. Matěj Grégr, Ph.D.

Autor:

Daniel Chudý (xchudy06)

Obsah

1 Uvedenie do problému

1.1 Úvod

NetFlow je protokol (vyvinutý spoločnosťou Cisco v roku 1996), ktorý umožňuje získavať informácie ohľadom sieťového prenosu, keď prichádza alebo odchádza z rozhrania. Analyzovaním získaných dát môže administrátor zistiť pôvod a destináciu prenosu, zápchu (úzke miesta) v prenose a jej pôvod, atď. NetFlow je užitočný pre poskytovateľov pripojenia, na údržbu a zabezpečenie siete.

1.2 NetFlow Architektúra

NetFlow architektúra sa typicky skladá z troch komponentov:

- **Exportér**: zoskupuje pakety do tokov (tzv. „flows“) a exportuje flows ich na kolektor
- Kolektor: zodpovedný za príjem, uchovávanie a predbežné spracovanie údajov o flows prijatých od exportéra
- Aplikácia na analýzu: analyzuje a vizualizuje dáta

Naším cieľom bolo implementovať práve **NetFlow exportér**.

1.3 Flows

Základ NetFlow architektúry je zoskupovanie podobných paketov do jedného toku (flow). Podobnosť paketov sa determinuje podľa pätice/sedmice údajov (v projekte sa používa označená **pätica**) :

1. Vstupné rozhranie (SNMP ifIndex)
2. **Zdrojová IP adresa**
3. **Cieľová IP adresa**
4. **IP protokol**
5. **Zdrojový port pre UDP alebo TCP, 0 pre ostatné protokoly**
6. **Cieľový port pre UDP alebo TCP, typ a kód pre ICMP alebo 0 pre iné protokoly**
7. IP Type of Service (ToS)

1.4 Verzia NetFlow

NetFlow je vydaný pod verziami v1 – v10, najpoužívanejšia je v5, ktorú využívame, je obmedzená na IPv4 toky.

1.5 NetFlow v5 formáty

Table B-3 Version 5 Header Format

Bytes	Contents	Description
0-1	version	NetFlow export format version number
2-3	count	Number of flows exported in this packet (1-30)
4-7	SysUptime	Current time in milliseconds since the export device booted
8-11	unix_secs	Current count of seconds since 0000 UTC 1970
12-15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970
16-19	flow_sequence	Sequence counter of total flows seen
20	engine_type	Type of flow-switching engine
21	engine_id	Slot number of the flow-switching engine
22-23	sampling_interval	First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval

Obrázok 1. : Formát hlavičky toku

Farebne vyznačené bajty nastavujeme na nuly. Tieto hodnoty nepoznáme, nedajú sa zistiť alebo sú padding.

Table B-4 Version 5 Flow Record Format

Bytes	Contents	Description
0-3	srcaddr	Source IP address
4-7	dstaddr	Destination IP address
8-11	nexthop	IP address of next hop router
12-13	input	SNMP index of input interface
14-15	output	SNMP index of output interface
16-19	dPkts	Packets in the flow
20-23	dOctets	Total number of Layer 3 bytes in the packets of the flow
24-27	First	SysUptime at start of flow
28-31	Last	SysUptime at the time the last packet of the flow was received
32-33	srcport	TCP/UDP source port number or equivalent
34-35	dstport	TCP/UDP destination port number or equivalent
36	pad1	Unused (zero) bytes
37	tcp_flags	Cumulative OR of TCP flags
38	prot	IP protocol type (for example, TCP = 6; UDP = 17)
39	tos	IP type of service (ToS)
40-41	src_as	Autonomous system number of the source, either origin or peer
42-43	dst_as	Autonomous system number of the destination, either origin or peer
44	src_mask	Source address prefix mask bits
45	dst_mask	Destination address prefix mask bits
46-47	pad2	Unused (zero) bytes

Obrázok 2. : Formát tela toku

2 Popis implementácie

2.1 Návrh

2.1.1 Spracovanie PCAP súboru

Projekt je rozdelený do niekoľkých logických častí. Na začiatku sa spracujú argumenty programu, pokračuje sa spracúvaním PCAP súboru pomocou knižnice **pcap.h**. Packety spracúvame offline, preto požijeme funkciu **pcap_open_offline( )**. Capture filter na „tcp or udp or icmp“, aby sme zachytávali len TCP, UDP a ICMP packety. Funkciou **pcap_loop( )** iterujeme cez zachytené packety, druhý argument nastavíme na -1, čím cyklíme nekonečne.

2.1.2 Spracovanie jednotlivých packetov

V „loopback“ funkcii **returned_packet( )** začíname so spracovaním daného packetu, nastavíme potrebné časy, ktoré potrebujeme pri NetFlow, skontrolujeme protokol sieťovej vrstvy (pri IPv6 protokole končíme program). Ďalej exportujeme potrebné flows, vkladáme nové alebo aktualizujeme existujúce. Export prevádzame pri vypršaní active/inactive časovačov, pri prekročení povolenej veľkosti flow cache a pri príchode TCP packetu s FIN/RST príznakom. Po spracovaní všetkých packetov (tj. po návrate z loopback funkcie) exportujeme zvyšok flow cache.

Flow cache je mapa typu **std::map** (globálna mapa **flow_map**)**,** kde ukladáme jednotlivé flows ako štruktúry. Kľúč mapy je definovaný ako **tuple**, konkrétne je to pätica **five_tuple**, spomínaná v sekcii 1.3.

Položky štruktúry s názvom **Nf_flow** sú naformátované podľa Obrázku 2. v sekcii 1.5. Deklarujeme jednu globálnu štruktúru **Nf_flow**, ktorá predstavuje telo toku. Takisto deklarujeme globálnu štruktúru **Nf_header**, ktorá predstavuje hlavičku exportu.

Vkladanie/aktualizovanie toku - najskôr sa zistí, či už podobný packet (packet so zhodnou päticou) neexistujte v mape ako flow. V kladnej vetve daný flow priamo v mape už len aktualizujeme (upravíme potrebné položky štruktúry). V opačnom prípade vytvoríme nový flow zmenením potrebných položiek globálnej štruktúry **Nf_flow**.

Exportovanie toku – pripraví sa hlavička zapísaním potrebných položiek vo funkcii **make_header( )**, exportuje sa daný flow (exportujeme vždy po jednom, tj. každý export je jeden flow a jedna hlavička, položka *count* v štruktúre hlavičky je vždy rovná 1) a daný flow sa vymaže z mapy.

2.1.3 Spracovanie IP hlavičky

Vo funkcii ipv4_fun( ) získavame zo štruktúry **iphdr** potrebné informácie na zostavenie kľúču do mapy, tj. pätice typu **tuple** a veľkosť danej IPv4 hlavičky (veľkosť je premenná). Zároveň determinujeme protokol transportnej vrstvy (TCP, UDP alebo ICMP, pri inom končíme program) a voláme príslušné funkcie, kde z daných hlavičiek získavame porty. Pri TCP packete navyše potrebujeme príznaky, **th_flags**. ICMP toky majú zdrojový port nulový, ale cieľový port sa počíta nasledovne: *dstport = type * 256 + code* (daný prístup som pre neexistujúcu citáciu zdroja v projekte len naznačil).

2.1.4 Exportovanie pomocou UDP klienta

Pri exporte bol použitý poskytnutý súbor „echo-udp-client2.c“ v E-Learningu, ktorý bol po úprave požitý na exportovanie NetFlow tokov na prípadný kolektor.

Vo funkcii **udp_export( )** sa okrem iného skopírujú štruktúry tela toku a hlavičky pomocou funkcie **memcpy( )**, ktorého obsah je po otvorení socketu odoslaný na kolektor.

3 Použitie

3.1 Návod na použitie

./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 kolektora. Voliteľne aj UDP port (127.0.0.1:2055, pokiaľ nie je špecifikované)

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

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

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

Všetky parametre sú brané ako voliteľné. Ak niektorý z parametrov nie je uvedený, použije sa namiesto neho východisková hodnota.

Príklad použitia:

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

3.2 Testovanie

Testovanie prebiehalo na Ubuntu-20.04 WSL pomocou nfdump, nfcapd a softlowd nástrojov nasledovne:

- zapnutie kolektoru pomocou nfcapd príkazom „nfcapd -T all -l . -I any -p 2055“
- spustenie programu napr. „./flow -f input.pcap“
- ukončíme načúvanie na kolektore pomocou CTRL + C
- vypíšeme si flows nfdump príkazom „nfdump -r nfcapd.2022xxxxxxxx“
- porovnanie výstupu s výstupom príkazu „softflowd -v 5 -n 127.0.0.1:2055 -r input.pcap

3.2.1 Ukážky testovania

Použitý postup z nadradenej kapitoly.

3.2.1.1 TCP s príznakom

Pcap súbor s TCP packetmi, obsahujúci FIN flag:

```
2022-10-07 18:59:32.929 INVALID  Ignore TCP       3.65.102.105:443   ->    100.69.167.92:53686
          0.0.0.0:0          372         0
2022-10-07 18:59:32.889 INVALID  Ignore TCP       3.65.102.105:443   ->    100.69.167.92:53694
          0.0.0.0:0          320         0
2022-10-07 18:59:44.755 INVALID  Ignore TCP     142.251.36.147:443   ->    100.69.167.92:38530
          0.0.0.0:0          381         0
2022-10-07 18:59:36.249 INVALID  Ignore TCP    142.250.102.188:5228  ->    100.69.167.92:46116
          0.0.0.0:0           52         0
2022-10-07 18:59:36.233 INVALID  Ignore TCP    162.159.129.232:443   ->    100.69.167.92:45596
          0.0.0.0:0           40         0
2022-10-07 18:59:25.561 INVALID  Ignore TCP    162.159.135.234:443   ->    100.69.167.92:59936
          0.0.0.0:0         2107         0
Summary: total flows: 28, total bytes: 17870, total packets: 105, avg bps: 7394, avg pps: 5, avg
Time window: 2022-10-07 18:59:25 - 2022-10-07 18:59:44
Total flows processed: 28, Blocks skipped: 0, Bytes read: 2368
```

Porovnanie s výstupom softflowd:

```
2022-10-07 18:59:32.853 INVALID  Ignore TCP       3.65.102.105:443   ->    100.69.167.92:53694
          0.0.0.0:0          324         0
2022-10-07 18:59:32.853 INVALID  Ignore TCP      100.69.167.92:53694 ->     3.65.102.105:443
          0.0.0.0:0          424         0
2022-10-07 18:59:33.994 INVALID  Ignore TCP      100.69.167.92:38530 ->   142.251.36.147:443
          0.0.0.0:0         4511         0
2022-10-07 18:59:33.994 INVALID  Ignore TCP     142.251.36.147:443   ->    100.69.167.92:38530
          0.0.0.0:0          720         0
Summary: total flows: 22, total bytes: 17938, total packets: 105, avg bps: 7423, avg pps: 5, av
Time window: 2022-10-07 18:59:25 - 2022-10-07 18:59:44
Total flows processed: 22, Blocks skipped: 0, Bytes read: 1888
Sys: 0.002s flows/second: 9799.6     Wall: 0.003s flows/second: 6684.9
```

Podľa výstupu som usúdil, že nástroj softflowd nepočíta s TCP príznakmi.

3.2.1.2 UDP

```
Date first seen          Event  XEvent Proto      Src IP Addr:Port          Dst IP Addr:Port
   X-Dst IP Addr:Port   In Byte Out Byte
2022-09-28 00:33:58.588 INVALID  Ignore UDP     100.64.216.215:54915 ->   100.64.223.255:54915
          0.0.0.0:0          582        0
2022-09-28 00:33:58.777 INVALID  Ignore UDP      100.64.195.73:54915 ->   100.64.223.255:54915
          0.0.0.0:0          582        0
2022-09-28 00:33:58.858 INVALID  Ignore UDP     100.64.192.180:54915 ->   100.64.223.255:54915
          0.0.0.0:0          582        0
2022-09-28 00:33:59.441 INVALID  Ignore UDP     10.190.100.195:34387 ->   10.190.103.255:5353
          0.0.0.0:0         1504        0
2022-09-28 00:33:59.609 INVALID  Ignore UDP     100.64.204.255:51437 ->   100.64.223.255:59870
          0.0.0.0:0          244        0
2022-09-28 00:33:59.615 INVALID  Ignore UDP     100.64.204.255:51439 ->   100.64.223.255:59870
          0.0.0.0:0          158        0
2022-09-28 00:34:00.211 INVALID  Ignore UDP     10.190.100.195:59970 ->   10.190.103.255:5353
          0.0.0.0:0         1606        0
2022-09-28 00:34:00.265 INVALID  Ignore UDP     100.64.192.223:57621 ->   100.64.223.255:57621
          0.0.0.0:0           72        0
Summary: total flows: 8, total bytes: 5330, total packets: 13, avg bps: 25426, avg pps: 7, avg
Time window: 2022-09-28 00:33:58 - 2022-09-28 00:34:00
Total flows processed: 8, Blocks skipped: 0, Bytes read: 768
Sys: 0.001s flows/second: 4461.8     Wall: 0.002s flows/second: 2733.2
```

Výstup s použitím nášho exportéra je zhodný s použitím softflowd.

Príkaz: ./flow -c localhost -m 3 -f nfDump/udp.pcap

Localhost sa správne preloží na 127.0.0.1 a počet flows sa dôsledkom zníženia kapacity flow cache navýši.

```
0.0.0.0:0          291        0
2022-09-28 00:33:59.441 INVALID  Ignore UDP     10.190.100.195:34387 ->   10.190.103.255:5353
          0.0.0.0:0         1504        0
2022-09-28 00:33:59.597 INVALID  Ignore UDP     100.64.216.215:54915 ->   100.64.223.255:54915
          0.0.0.0:0          291        0
2022-09-28 00:33:59.609 INVALID  Ignore UDP     100.64.204.255:51437 ->   100.64.223.255:59870
          0.0.0.0:0          244        0
2022-09-28 00:33:59.615 INVALID  Ignore UDP     100.64.204.255:51439 ->   100.64.223.255:59870
          0.0.0.0:0          158        0
2022-09-28 00:33:59.775 INVALID  Ignore UDP      100.64.195.73:54915 ->   100.64.223.255:54915
          0.0.0.0:0          291        0
2022-09-28 00:33:59.858 INVALID  Ignore UDP     100.64.192.180:54915 ->   100.64.223.255:54915
          0.0.0.0:0          291        0
2022-09-28 00:34:00.211 INVALID  Ignore UDP     10.190.100.195:59970 ->   10.190.103.255:5353
          0.0.0.0:0         1606        0
2022-09-28 00:34:00.265 INVALID  Ignore UDP     100.64.192.223:57621 ->   100.64.223.255:57621
          0.0.0.0:0           72        0
Summary: total flows: 11, total bytes: 5330, total packets: 13, avg bps: 25426, avg pps: 7, avg
Time window: 2022-09-28 00:33:58 - 2022-09-28 00:34:00
Total flows processed: 11, Blocks skipped: 0, Bytes read: 1008
Sys: 0.005s flows/second: 2065.3     Wall: 0.002s flows/second: 3776.2
```

3.2.1.3 ICMP

```
Date first seen          Event  XEvent Proto      Src IP Addr:Port          Dst IP Addr:Port
   X-Dst IP Addr:Port   In Byte Out Byte
2022-09-28 00:32:50.126 INVALID  Ignore ICMP    100.64.208.103:0     ->    66.254.114.41:0.0
          0.0.0.0:0          168        0
2022-09-28 00:32:50.137 INVALID  Ignore ICMP     66.254.114.41:0     ->   100.64.208.103:0.0
          0.0.0.0:0          168        0
Summary: total flows: 2, total bytes: 336, total packets: 4, avg bps: 2643, avg pps: 3, avg b
Time window: 2022-09-28 00:32:50 - 2022-09-28 00:32:51
Total flows processed: 2, Blocks skipped: 0, Bytes read: 288
Sys: 0.001s flows/second: 1084.0     Wall: 0.002s flows/second: 736.1
```

Výstup s použitím nášho exportéra je zhodný s použitím softflowd.

3.2.1.4 Väčší PCAP súbor s použitím časovačov

Bez použitia časovačov je výstup zhodný s programom softflowd.

```
^CIdent: 'any' Flows: 67, Packets: 2461, Bytes: 2602324, Sequence Errors: 0, Bad Packets: 0
Total ignored packets: 0
Terminating nfcapd.
```

Príkaz: ./flow -f input.pcap -i 5 -a 10 -m 5

Počet flows sa navýši skoro dvojnásobne.

```
^CIdent: 'any' Flows: 134, Packets: 2461, Bytes: 2602324, Sequence Errors: 0, Bad Packets: 0
Total ignored packets: 0
Terminating nfcapd.
```

4 Literatúra

Cartens, T.: PROGRAMMING WITH PCAP, webová lokalita [online], [cit. 2022-12-11]. Dostupné z: https://www.tcpdump.org/pcap.html

Wikipedia: NetFlow, webová lokalita [online], [cit. 2022-12-11]. Dostupné z: https://en.wikipedia.org/wiki/NetFlow#Records

Cisco: NetFlow Export Datagram Format, webová lokalita [online], [cit. 2022-12-11]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/net_mgmt/netflow_collection_engine/3-6/user/guide/format.html#wp1003394