



Síťové aplikace a správa sítí
2022/2023

Dokumentace k projektu
Generování NetFlow dat ze zachycené síťové
komunikace

Autor:

David Drtil (xdrtil03)

Brno, 11. listopadu 2022

Obsah

Úvod	3
Detailní popis implementace	3
Kontrolní výpisy o exportování NetFlows	4
Pomocná funkce	4
Ukázky použití exportéru a testování	4
Testovací metody:	4
Citace použitých zdrojů.....	7

Úvod

Cílem bylo navrhnout a naimplementovat NetFlow exportér, který je schopný zpracovat zachycený síťový provoz ve formátu pcap, z nich vytvořit NetFlow záznamy a ty následně odeslat na kolektor. Tento proces se používá za účelem identifikování provozu v síti pro další analýzu jako je zjištění, zda je síťová infrastruktura dostatečně robustní, nebo také pro rozpoznání nekalých činností (útoků), které někdo může v síti páchat.

Detailní popis implementace

NetFlow analyzátor byl naimplementován v jazyce C s využitím síťových knihoven pcap a netinet a podporuje export pouze NetFlow v5 datagramů [1]. Pro definování NetFlows je zvolen jako klíč pětkice (5-tuple) <protocol, src_ip, src_port, dst_ip, dst_port> podle Cisco ASA [2] na místo sedmice (7-tuple) <protocol, src_ip, src_port, dst_ip, dst_port, ip_tos, interface_ifIndex>.

Po spuštění programu dojde ve funkci `main()` k volání funkce `handle_sigint()` zachytávající systémové přerušení (např. Ctrl + C) pro bezpečné ukončení programu a uvolnění všech alokovaných zdrojů.

Následně probíhá načtení argumentů do struktury `args_t` a jejich kontrola ve funkci `parse_arguments()`, zda jsou syntakticky správné. Vytvoří se cache implementovaná pro svou jednoduchost dvousměrně vázaným seznamem. Otevře se udp socket pro odesílání exportovaných NetFlow na kolektor, otevře se pcap soubor a v hlavní smyčce programu, funkci `process_pcap_file()`, začne zpracování zachyceného síťového provozu. Brány v potaz jsou pouze pakety s protokolem TCP, UDP a ICMP, ostatní jsou odfiltrovány display filtrem pomocí funkce `pcap_setfilter()`

Původní časové značky paketů ze souboru jsou ukládány do 64bitového čísla. Důležitý je časový údaj prvního příchozího paketu, který se považuje za čas 0, a pomocí něj se poté počítá čas příchodu dalších paketů. Po načtení časového údaje je zkontrolováno, zda nešlo k překročení doby aktivního a neaktivního intervalu NetFlow v cache funkcí `check_timers()`.

Po načtení klíče Netflow z hlaviček příchozího paketu se rozhoduje, zda má být paket agregován do existujícího NetFlow nebo má být založen nový NetFlow. Při agregaci k existujícímu NetFlow jsou kontrolovány „tcp flags“, pokud je nastaven flag FIN nebo RST [3] je NetFlow exportován a nečeká se na vypršení neaktivního časovače.

Po zpracování posledního paketu z pcap souboru, dojde k ukončení hlavní smyčky programu, exportování všech zbývajících NetFlows z cache, uvolní se paměť všech alokovaných struktur, uzavře se socket a soubor zavoláním funkce `cleanup_on_exit()`.

Kontrolní výpisy o exportování NetFlows

Program je navržený tak, aby se pomocí logů vypisovaných na příkazovou řádku dalo zjistit, jak zpracování souboru a export NetFlow probíhalo. Tyto výpisy lze jednoduše vypnout pomocí nastavení preprocesoru `LOG_NETFLOWS_PROCESSING_ENABLED` na hodnotu `false`. V odevzdané verzi je výpis povolen.

Pomocná funkce

Funkce `get_readable_ipv4_address()` zpracovává v jednoduchém cyklu 32bitové číslo extrahované ze struktury `ip_header` a toto číslo načte ve správném formátu pro výpis do předaného pole.

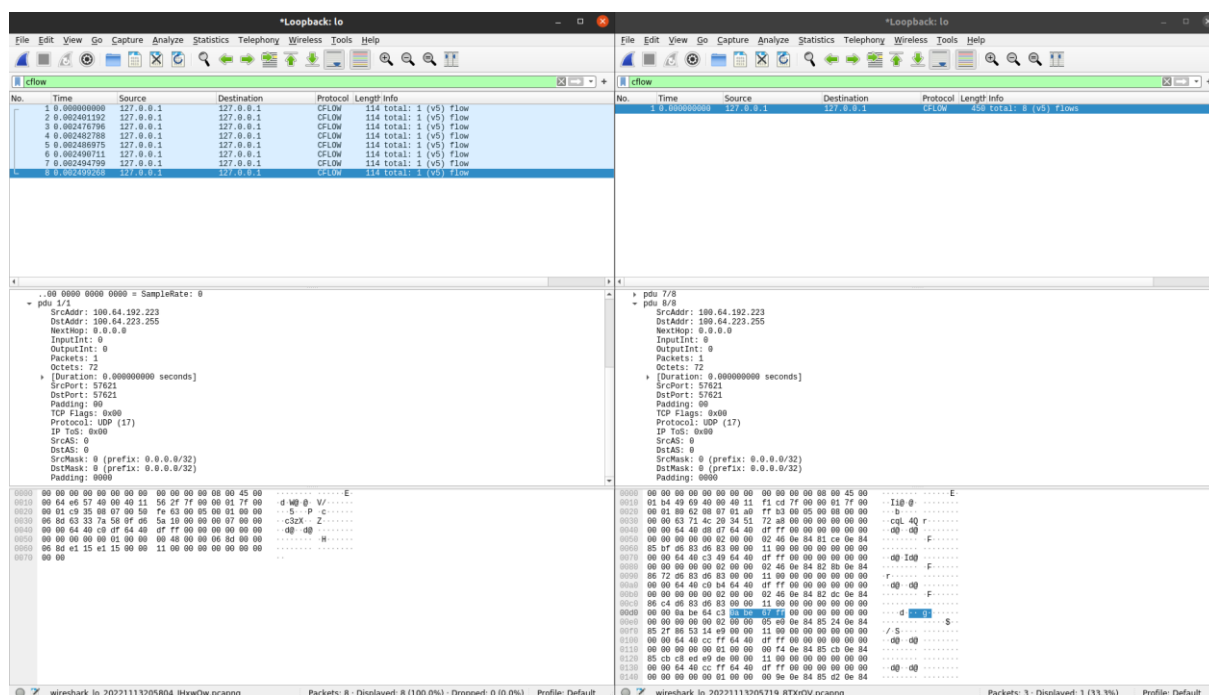
Ukázky použití exportéru a testování

Pomocí programu `tcpdump` jsem zachycoval síťovou komunikaci a vytvořil testovací soubory s formátem `pcap` (příponou `.pcap`).

Testovací metody:

- 1) Vlastní NetFlow exportér jsem spouštěl s testovacími soubory a posílal jsem vytvořené NetFlow datagramy verze 5 na adresu `0.0.0.0:2055`, což je adresa pro zachytávání Cisco NetFlow [4]. Exportované NetFlow jsem zachytil aplikací Wireshark, která odposlouchávala na rozhraní „lo“ (loopback) a měla nastavený display filtr na „cflow“. Následně jsem zachytil v aplikaci Wireshark také referenční výstup z veřejně dostupného exportéru „softflowd“ a srovnal jsem výstupy s mými exportovanými NetFlow pro ověření správnosti.

Příkaz – „`sudo softflowd -v 5 -n 0.0.0.0:2055 -r ./pcap_test_files/captured_traffic.pcap`“



Obrázek č. 1 – Srovnání poslaných datagramů vlastního NetFlow exportéru s výstupem softflowd sw

- 2) Pomocí programu „nfcapd“ jsem vytvořil kolektor neboli udp server běžící na zadaném portu. Na kolektor jsem posílal vlastní NetFlow datagramy a referenční NetFlow datagramy pomocí již zmiňovaného programu „softflowd“. Kolektor každých 5 minut vytvořil ze zachycených NetFlow datagramů soubor čitelný programem nfdump a vytvořit souhrny, které jsem následně pomocí programu diff porovnával.

Příkaz – „nfcapd -D -T all -l . -l any -S 2 -p 20549 & sudo sudo softflowd -v 5 -n 0.0.0.0:20549 -r ./pcap_test_files/captured_traffic.pcap“

```

davidrttl@davidrttl-VirtualBox: ~/Desktop/ISA_project/2022/11/13/21$ nfdump -r ./nfcapd.202211132143
Date first seen      Event XEvent Proto  Src IP Addr:Port  Dst IP Addr:Port  In Byte Out Byte
2022-09-28 00:33:58.588 INVALID Ignore UDP  0.0.0.0:0 -> 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 582 0
2022-09-28 00:33:58.857 INVALID Ignore UDP  100.64.192.180:54915 -> 100.64.223.255:54915 582 0
2022-09-28 00:33:59.441 INVALID Ignore UDP  10.190.100.195:34387 -> 10.190.103.255:5353 1504 0
2022-09-28 00:33:59.608 INVALID Ignore UDP  100.64.204.255:51437 -> 100.64.223.255:59870 244 0
2022-09-28 00:33:59.615 INVALID Ignore UDP  100.64.204.255:51439 -> 100.64.223.255:59870 158 0
2022-09-28 00:34:00.211 INVALID Ignore UDP  10.190.100.195:59970 -> 10.190.103.255:5353 1606 0
2022-09-28 00:34:00.265 INVALID Ignore UDP  100.64.192.223:57621 -> 100.64.223.255:57621 72 0
Summary: total flows: 8, total bytes: 5330, total packets: 13, avg bps: 25426, avg pps: 7, avg b
pp: 418
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: 5633.8 Wall: 0.000s flows/second: 70796.5
davidrttl@davidrttl-VirtualBox: ~/Desktop/ISA_project/2022/11/13/21$

davidrttl@davidrttl-VirtualBox: ~/Desktop/ISA_project/2022/11/13/21$ nfdump -r ./nfcapd.202211132148
Date first seen      Event XEvent Proto  Src IP Addr:Port  Dst IP Addr:Port  In Byte Out Byte
2022-09-28 00:33:58.587 INVALID Ignore UDP  0.0.0.0:0 -> 0.0.0.0:0 582 0
2022-09-28 00:33:58.776 INVALID Ignore UDP  100.64.195.73:54915 -> 100.64.223.255:54915 582 0
2022-09-28 00:33:58.857 INVALID Ignore UDP  100.64.192.180:54915 -> 100.64.223.255:54915 582 0
2022-09-28 00:33:59.441 INVALID Ignore UDP  10.190.100.195:34387 -> 10.190.103.255:5353 1504 0
2022-09-28 00:33:59.608 INVALID Ignore UDP  100.64.204.255:51437 -> 100.64.223.255:59870 244 0
2022-09-28 00:33:59.615 INVALID Ignore UDP  100.64.204.255:51439 -> 100.64.223.255:59870 158 0
2022-09-28 00:34:00.211 INVALID Ignore UDP  10.190.100.195:59970 -> 10.190.103.255:5353 1606 0
2022-09-28 00:34:00.265 INVALID Ignore UDP  100.64.192.223:57621 -> 100.64.223.255:57621 72 0
Summary: total flows: 8, total bytes: 5330, total packets: 13, avg bps: 25411, avg pps: 7, avg b
pp: 418
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: 5610.1 Wall: 0.000s flows/second: 73394.5
davidrttl@davidrttl-VirtualBox: ~/Desktop/ISA_project/2022/11/13/21$

```

Obrázek č. 2 – Srovnání výstupů programu nfdump

- 3) Testování na školním serveru Merlin probíhalo tím způsobem, že jsem zde otestoval, zda je program možné přeložit a spustit. Následně jsem porovnal údaje z výpisu / logů činnosti NetFlow exportéru na stroji běžícím na OS Ubuntu 20.04. Zde jsem ale musel posílat datagramy na jednu adresu, které byly již aktivní. K vyhledání takové adresy jsem použil příkaz „netstat -n --udp --listen“.

```

merlin.fit.vutbr.cz - PuTTY
xdrtil03@merlin: ~/3_rocnik/ISA project$ ./flow -c 0.0.0.0:41808 -f ./pcap_files/tcp-fin.pcap
Inserted 1. nf with: 162.159.135.234:47873 -> 100.69.167.92:8426
Inserted 2. nf with: 100.69.167.92:8426 -> 162.159.135.234:47873
Inserted 3. nf with: 100.69.167.92:26784 -> 104.70.109.120:47873
Inserted 4. nf with: 104.70.109.120:47873 -> 100.69.167.92:26784
Inserted 5. nf with: 100.69.167.92:57472 -> 107.23.110.60:47873
Inserted 6. nf with: 107.23.110.60:47873 -> 100.69.167.92:57472
Inserted 7. nf with: 192.0.73.2:47873 -> 100.69.167.92:36021
Inserted 8. nf with: 100.69.167.92:36021 -> 192.0.73.2:47873
Due to obtaining fin flag:
Exported 1. nf with: 192.0.73.2:47873 -> 100.69.167.92:36021
Due to obtaining fin flag:
Exported 2. nf with: 100.69.167.92:36021 -> 192.0.73.2:47873
Inserted 9. nf with: 192.0.73.2:47873 -> 100.69.167.92:36021
Inserted 10. nf with: 100.69.167.92:3262 -> 142.251.36.74:47873
Inserted 11. nf with: 142.251.36.74:47873 -> 100.69.167.92:3262
Inserted 12. nf with: 100.69.167.92:46801 -> 3.65.102.105:47873
Inserted 13. nf with: 100.69.167.92:48849 -> 3.65.102.105:47873
Inserted 14. nf with: 3.65.102.105:47873 -> 100.69.167.92:48849
Inserted 15. nf with: 3.65.102.105:47873 -> 100.69.167.92:46801
Inserted 16. nf with: 100.69.167.92:33430 -> 142.251.36.147:47873
Inserted 17. nf with: 142.251.36.147:47873 -> 100.69.167.92:33430
Inserted 18. nf with: 100.69.167.92:7346 -> 162.159.129.232:47873
Inserted 19. nf with: 100.69.167.92:9396 -> 142.250.102.188:27668
Inserted 20. nf with: 162.159.129.232:47873 -> 100.69.167.92:7346
Inserted 21. nf with: 142.250.102.188:27668 -> 100.69.167.92:9396
Due to expiration of INActive timer:
Exported 3. nf with: 100.69.167.92:26784 -> 104.70.109.120:47873
Due to expiration of INActive timer:
Exported 4. nf with: 104.70.109.120:47873 -> 100.69.167.92:26784
Inserted 22. nf with: 100.69.167.92:3774 -> 142.251.36.74:47873
Inserted 23. nf with: 142.251.36.74:47873 -> 100.69.167.92:3774
Due to expiration of INActive timer:
Exported 5. nf with: 100.69.167.92:57472 -> 107.23.110.60:47873
Due to expiration of INActive timer:
Exported 6. nf with: 107.23.110.60:47873 -> 100.69.167.92:57472

```

Obrázek č. 3 – Výpis zpracování NetFlows na školním serveru Merlin

```
daviddrttil@daviddrttil-VirtualBox: ~/Desktop/ISA_project
daviddrttil@daviddrttil-VirtualBox:~/Desktop/ISA_project$ ./flow -f ./pcap_files/tcp-fin.pcap -c 0.0.0.0:2055
Inserted 1. nf with: 162.159.135.234:47873 -> 100.69.167.92:8426
Inserted 2. nf with: 100.69.167.92:8426 -> 162.159.135.234:47873
Inserted 3. nf with: 100.69.167.92:26784 -> 104.70.109.120:47873
Inserted 4. nf with: 104.70.109.120:47873 -> 100.69.167.92:26784
Inserted 5. nf with: 100.69.167.92:57472 -> 107.23.110.60:47873
Inserted 6. nf with: 107.23.110.60:47873 -> 100.69.167.92:57472
Inserted 7. nf with: 192.0.73.2:47873 -> 100.69.167.92:36021
Inserted 8. nf with: 100.69.167.92:36021 -> 192.0.73.2:47873
Due to obtaining fin flag:
Exported 1. nf with: 192.0.73.2:47873 -> 100.69.167.92:36021
Due to obtaining fin flag:
Exported 2. nf with: 100.69.167.92:36021 -> 192.0.73.2:47873
Inserted 9. nf with: 192.0.73.2:47873 -> 100.69.167.92:36021
Inserted 10. nf with: 100.69.167.92:3262 -> 142.251.36.74:47873
Inserted 11. nf with: 142.251.36.74:47873 -> 100.69.167.92:3262
Inserted 12. nf with: 100.69.167.92:46801 -> 3.65.102.105:47873
Inserted 13. nf with: 100.69.167.92:48849 -> 3.65.102.105:47873
Inserted 14. nf with: 3.65.102.105:47873 -> 100.69.167.92:48849
Inserted 15. nf with: 3.65.102.105:47873 -> 100.69.167.92:46801
Inserted 16. nf with: 100.69.167.92:33430 -> 142.251.36.147:47873
Inserted 17. nf with: 142.251.36.147:47873 -> 100.69.167.92:33430
Inserted 18. nf with: 100.69.167.92:7346 -> 162.159.129.232:47873
Inserted 19. nf with: 100.69.167.92:9396 -> 142.250.102.188:27668
Inserted 20. nf with: 162.159.129.232:47873 -> 100.69.167.92:7346
Inserted 21. nf with: 142.250.102.188:27668 -> 100.69.167.92:9396
Due to expiration of INactive timer:
Exported 3. nf with: 100.69.167.92:26784 -> 104.70.109.120:47873
Due to expiration of INactive timer:
Exported 4. nf with: 104.70.109.120:47873 -> 100.69.167.92:26784
Inserted 22. nf with: 100.69.167.92:3774 -> 142.251.36.74:47873
Inserted 23. nf with: 142.251.36.74:47873 -> 100.69.167.92:3774
Due to expiration of INactive timer:
Exported 5. nf with: 100.69.167.92:57472 -> 107.23.110.60:47873
Due to expiration of INactive timer:
Exported 6. nf with: 107.23.110.60:47873 -> 100.69.167.92:57472
```

Obrázek č. 4 – Výpis zpracování NetFlows na OS Ubuntu 20.04

Citace použitých zdrojů

- [1] Cisco NetFlow export datagram formats [online]. Kalifornie (USA): Cisco Systems, 2007 [cit. 2022-11-13]. Dostupné z:
https://www.cisco.com/c/en/us/td/docs/net_mgmt/netflow_collection_engine/3-6/user/guide/format.html
- [2] NetFlow identification key [online]. Cisco community [cit. 2022-11-13]. Dostupné z:
<https://community.cisco.com/t5/security-knowledge-base/netflow-on-asa/ta-p/3119176>
- [3] TCP flags decoding [online]. Manito Networks [cit. 2022-11-13]. Dostupné z:
<https://www.manitonetworks.com/flow-management/2016/10/16/decoding-tcp-flags>
- [4] Cisco NetFlow default ports [online]. NSRC [cit. 2022-11-13]. Dostupné z:
https://nsrc.org/workshops/2017/sanog29-cndo/networking/cndo/en/presentations/9.2_Netflow.pdf