

Projekt ISA - PCAP NetFlow v5 exportér

Obsah

1 Teória	3
1.1 Prehľad	3
1.2 Timeout	3
2 Implementácia programu p2nprobe.....	3
2.1 flow_aggregator.h.....	3
2.2 netflow_v5_structure.h	3
2.3 p2nprobe.cpp.....	3
3 Testovanie	4
3.1 Výsledky testovania	4

1 Teória

1.1 Prehľad

Program p2nprobe slúži na spracovanie sieťových tokov z PCAP súborov a export ich informácií vo formáte NetFlow v5 na kolektor prostredníctvom protokolu UDP. NetFlow je protokol používaný na zber informácií o sieťovej prevádzke, pričom záznamy o tokoch predstavujú agregované údaje o komunikácii medzi dvojicami IP adries. Tieto záznamy obsahujú informácie ako zdrojová a cieľová IP adresa, porty, objem prenesených dát a ďalšie štatistiky o toku. Program spracováva iba TCP prevádzku, čím sa zjednodušuje implementácia, nakoľko sa vynecháva napríklad UDP a iné protokoly. Export záznamov sa vykonáva až po skončení agregácie toku na základe časového timeoutu alebo ukončenia relácie.

1.2 Timeout

Active a inactive timeout sú mechanizmy používané pri správe sieťových tokov v nástrojoch, ako je NetFlow.

Active timeout určuje, ako dlho bude tok aktívny a pravidelne reportovaný, aj keď stále prebieha. Po uplynutí tejto doby sa tok uzavrie a vygeneruje sa záznam, aj keď komunikácia medzi zariadeniami stále prebieha. Tento mechanizmus umožňuje pravidelné monitorovanie dlhodobých tokov.

Inactive timeout sa používa na detekciu ukončenia toku. Ak sa počas tohto časového intervalu nezaznamená žiadna aktivita (napr. nové pakety pre daný tok), tok sa považuje za ukončený a je vytvorený záznam o jeho stave.

Tieto timeouty umožňujú efektívne spravovanie toku dát a predchádzajú nadmernému oneskoreniu v reportovaní o sieťovej prevádzke.

2 Implementácia programu p2nprobe

Program p2nprobe sa skladá z 3 súborov: flow_aggregator.h, netflow_v5_structure.h, p2nprobe.cpp a k nim priložený makefile.

2.1 flow_aggregator.h

Súbor flow_aggregator.h obsahuje štruktúru pre identifikáciu toku a štruktúru pre uchovanie štatistík o danom toku.

2.2 netflow_v5_structure.h

Súbor netflow_v5_structure.h dve štruktúry potrebné pre vytvorenie NetFlow v5 správy. Jedna pre hlavičku a druhá pre telo – samotný záznam o toku.

2.3 p2nprobe.cpp

Súbor p2nprobe.cpp obsahuje implementáciu logiky a fungovania celého programu. Skladá sa z niekoľkých funkcií: main, kde sa načítajú vstupné argumenty programu, nastaví sa dôležité

premenné, ako je cesta k pcap súboru, IP adresa a port kolektoru, active a inactive timeout. Následne sa nastaví socket na odosielanie dát a prejde sa do funkcie `read_pcap_file`. V tejto funkcii sa prečítajú jednotlivé pakety, ktoré ďalej postupujú do funkcie `process_packet`. Táto funkcia iba prefiltruje jednotlivé pakety tak, aby zostali iba TCP pakety, ktoré sa neskôr spracujú vo funkcii `process_tcp_packet`. Vo funkcii `process_tcp_packet` sa potom vytvárajú nové, alebo upravujú existujúce záznamy o tokoch, ktoré sa na konci odosielať pomocou UDP správ na kolektor. Pri vytváraní záznamov sa prevádza kontrola na active a inactive timeout, a naplnenie NetFlow správy, teda maximálne 30 záznamov. Po splnení tejto podmienky sa správa odošle na kolektor. Po prečítaní menej ako 30 záznamov a ukončení pcap súboru sa ešte vo funkcii `read_pcap_file` na konci skontroluje, či neostali nejaké neodoslané záznamy a odošlú sa na kolektor. V súbore `p2nprobe.cpp` sa ďalej nachádza aj pár pomocných funkcií, ako je napríklad funkcia na kontrolu platnosti vstupných argumentov, alebo výpis pomoci.

3 Testovanie

Pomocou programu `nfcapd` bol vytvorený server na prijímanie NetFlow správ. Na tento server sa pomocou programu `softflowd` posielali spracované záznamy o TCP tokoch z pcap súborov, a následne sa z tých istých pcap súborov vytvorili záznamy o TCP tokoch a poslali pomocou NetFlow správ aj z testovaného programu `p2nprobe`. Výsledné výstupy z obidvoch postupov sa nakoniec zobrazili pomocou `nfdupm -r` a porovnali medzi sebou.

3.1 Výsledky testovania

Testovanie bolo prevedené pomocou vyššie popísaného postupu, a výsledky testov dokázali zhodu medzi referenčným výstupom, generovaným pomocou programu `softflowd` a kontrolovaným výstupom programu `p2nprobe`.