Dokumentácia k projektu z predmetu ISA

Offline netflow sonda

22.11. 2015

Matúš Ondris (xondri04)

Zadanie:

Implementujte analyzátor zachycené síťové komunikace ve formátu PCAP, který bude fungovat jako offline NetFlow sonda (*exporter).*

NetFlow sonda je typicky síťový prvek, který agreguje informace o průchozí komunikaci do *flows*. Datové pakety patřící do stejného *flow* jsou identifikovány podle pětice položek - zdrojová/cílová IP adresa, zdrojový/cílový port a typ transportního protokolu. Informace o jednotlivých *flow* jsou exportovány sondou v NetFlow datagramu na NetFlow kolektor. NetFlow datagram může obsahovat informace o více *flow.* Sonda může odesílat data na kolektor buď v pravidelném intervalu, nebo po dosažení určitého množství flow v lokální paměti.

Vaším úkolem je tedy implementovat nástroj, který analyzuje zachycenou komunikaci a vyexportuje ji na kolektor ve formátu NetFlow v5.

Rozbor požiadavkou:

Zo zadanie je zrejmé , že program bude nutné rozdeliť na niekoľko menších problémov , ktoré budú navzájom komunikovať. V prvom rade je potrebné správne spracovať parametre príkazového riadku. Potom je potrebné načítať PCAP záznamy , ktoré získame buď zo zadaného .pcap súboru , alebo zo stdin na základe zadaného resp. nezadaného parametru -i <file> z argumentov programu. Ďalej je potrebné pakety zaznamenané v PCAP analyzovať a roztriediť do flows, jednotlivé flows je nutné skontrolovať , či (v prípade tcp) už komunikácia nebola expirovaná , tj parameter -t [--tcp-timeout] bol dosiahnutý, alebo flows už sú spracovávané a teda je nutné pristúpiť k nim do pamäte , kde sa nachádzajú a aktualizovať potrebné informácie. Na koniec záznamy o flows nutńe exportovať na kolektor , pokiaľ počet záznamov dosiahol hodnotu parametru -m [--max-flows] , alebo vypršal interval -I [--interval] , alebo došlo k spracovaniu celého PCAP záznamu a v pamäti ostali flows , ktoré je potrebné odoslať na kolektor.

Protokol NetFlow v5:

Dokumentácia viz.:
http://www.cisco.com/en/US/docs/ios/solutions_docs/netflow/nfwhite.html
Netflow v5 je proprietální protokol pre zasielanie informácií o 'flows' na 'kolektor'. Je však veľmi rozšírený. Tok je definovaný ako množina paketov, ktoré prešli rozhraním v určitom časovom rozpätí v jednom smere a majú rovnaké kľúčové parametre. NetFlow v5 pakety sa posielajú cez UDP.
Tu sú dostupné kľúčové parametre:
• Zdrojová a cieľová IP adresa (Ipv4)
• Zdrojový a cieľový port
• IP Protokol (TCP/UDP/ICMP/...)
• IP TOS (Type Of Service)
Štruktúra NetFlow v5 paketu je popísaná tu:
https://en.wikipedia.org/wiki/NetFlow
Toky sa exportujú hlavne podľa toho, kedy přišiel prvý a posledný paket. Ďalším kritériom môže byť podrobnejší rozbor TCP komunikácie alebo přetečítanie hodnôt vo FLOW RECORD. Úlohou je teda vytvárať flows zo zachytených paketov a tie potom vkladať do NetFlow datagramu, ktorý sa posiela na kolektor.

Popis implementácie:

Na začiatok chcem spomenúť , že implementácia a funkčnosť môjho exportéra nieje kompletná. Nefunguje odosielanie flows na kolektor a čítanie zo stdin. Nenaimplementoval sim ich kvôli zlému rozloženiu času z mojej strany.
Hlavičkový súbor exporter.h obsahuje:

Štruktúry :

- Params – slúži na uloženie spracovaných parametrov príkazového riadnu
- Nfv5_head – slúži na získanie a doplnenie Netflowv5 hlavičky pred odosielaním na kolektor.
- Nflowv5_body slúži na uloženie informácií o tele flows.

Hlavný súbor exporter.cpp slúži na spracovanie parametrov príkazového riadku pomocou funkcie getopts . Offline otvorenie zadaného.pcap súboru a cyklické prechádzanie paketov v súbore. Pakety triedim do flows a napĺňam ich požadovanými hodnotami. Ďalej kontrolujem , či nedošlo k niektorému z parametrov pre odoslanie flows na kolektor , alebo v prípade tcp nevypršal tcp timeout. Kontrolujem , či spracovávaný paket už nieje reprezentovaný vo vektore flows_arr , ak tam je tak doplním informácie k danému paketu , ak tam nieje , tak paket pridám do vektoru flow_arr.
Na koniec by mala byť funkcia , ktorá odosiela flows na kolektor, ktorú som nenaimplementoval.

Návod k použitiu:

Program sa prekladá z terminálu pomocou príkazu make.
Program sa spúšťa z terminálu pomocou príkazu :
./isa_esporter <parametre>
Popis parametrov:
–h - zobrazí nápovedu.
-i <file> slúži na zadanie vstupného .pcap súboru , v prípade nezadania pracuje zo stdin.
-c <neflow_collector:port> Adresa a port kolektoru , v prípade nezadania sa používa **127.0.0.1:2055.**
-I <interval>Reprezentuje časový interval , po ktorého uplynutí exportuje flows z pamäti na kolektor implicitne **300** sekúnd
-m <count> Reprezentuje počet záznamov v pamäti exportéra, po ktorých dosiahnutí exportuje flows z pamäti na kolektor implicitne **50** záznamov.
-t <seconds> Reprezentuje časový interval , po ktorého uplynutí exportuje sa považuje tcp spojenie za ukončené implicitne **300** sekúnd.

Příklad použitia:
./isa_exporter -i test_output_file.pcap -c 127.0.0.1:2055 Bude spracovávať flows zo súboru test_output_file.pcap a bude ich exportovať na kolektor 127.0.0.1 s portom 2055.

Referencie:

https://wis.fit.vutbr.cz/FIT/st/course-sl.php?id=588260&item=54115&nc=1 (zadanie vo WISe)
https://en.wikipedia.org/wiki/NetFlow (Popis flows)
http://www.cisco.com/c/en/us/td/docs/net_mgmt/netflow_collection_engine/3-6/user/guide/format.html# (popis tela a hlavicky ipv5 datagramu)
manuálové man stránky.