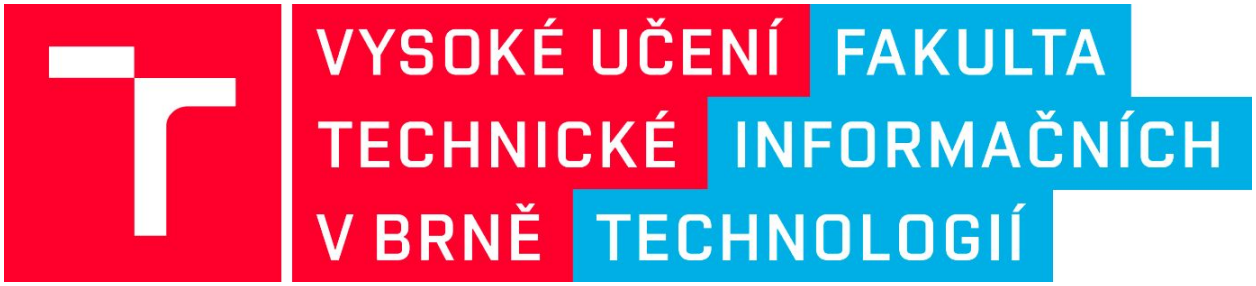
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



Dokumentace k projektu do předmětu ISA

Detekce aplikací generující síťový provoz

16. října 2016

Autor: Petr Nodžák, xnodza00@stud.fit.vutbr.cz
Fakulta Informačních Technologií
Vysoké Učení Technické v Brně

Obsah

1 Úvod

Tato dokumentace vznikla k projektu do předmětu Síťové aplikace a správa sítí. Dokument ve zkratce popisuje návrh, implementaci a použití výsledné aplikace. Tato aplikace může být využívána pro sledování síťového provozu určitých aplikací.

2 Důležité pojmy

2.1 Monitorování síťového toku

Hlavním účelem je monitorování síťového provozu na základě IP toků, které poskytuje podrobný pohled do provozu na síti v reálném čase. Proto tvoří důležitou a nepostradatelnou součást zabezpečení každé počítačové sítě a je užitečný pro poskytovatele připojení, kteří na základě statistik z monitorování síťového toku mohou svým zákazníkům účtovat ceny služeb v závislosti na množství přenesených dat. Lze s němi odhalovat vnější i vnitřní incidenty, úzká místa v síti, dominantní zdroje provozu, efektivněji plánovat budoucí rozvoj sítě, sledovat, kdo komunikoval s kým, jak dlouho a s pomocí kterého protokolu[1].

3 Implementace

Program je implementován v jazyce C++. Aplikace využívá některých objektů ze standardních knihoven jazyka C++. Aplikace je vytvořena pro OS Linux, byla vyvýjena a testována na Ubuntu 14.04

3.1 Parsování všech spojení

Funkce ***check()*** jako parametr dostane jméno aplikace, kterou má kontrolovat. Následně se zavolá funkce ***popen()*** s příkazem ***"lsof -Pnl -i4 -i6"***, který vypíše seznam informací o všech otevřených souborech a procesech, které je otevřely[2]. Přepínač ***-P*** zajistí, že nepřemění číslo portu na název síťového souboru, přepínač ***-n*** zajistí, že nepřemění IP adresu na název síťovéo souboru, přepínač ***-l*** zajistí, že nepřemění identifikační čísla uživatelů na jejich přihlašovací jména, přepínač ***+M*** povolí oznamování portmapper pro TCP, UDP. Přepínač -i4 a -i6 zajistí, že se budou zobrazovat jen adresy IPv4 a IPv6.
Dále se vybírají řádky z file descriptoru, který nám vrátila funkce ***popen()***. Z těchto řádků se parsují důležité informace a uloží do struktury, jako je zdrojová použitý protokol, zdrojová IP adresa, zdrojový port, cílová IP adresa, cílový port. Následně se prochází seznam takto vytvořených struktur, kde se aktualizují stavy spojení, které určí, co se se spojením bude následně dít.

3.2 Procházení všech spojení

Program běží v nekonečné smyčce, ve které volá funkci ***check()***, ta naplní seznam spojení, u kterých se kontrolují stavy. Pokud je ve struktuře nastavená proměnná ***active*** na false, už neprobíhá síťový provoz, tak se vymaže ze seznamu spojení. Pokud je nastavená proměnná ***printable*** na true, spojení nově přibilo do seznamu spojení, vypíše/odešle se. Na konec se celá smyčka uspí po dobu intervalu zadaného od uživatele.

3.3 Odesílání zpráv

Funkce ***sendLog()*** vytvoří a odešle socket se zprávou ve formátu "protokol zdrojováIP zdrojovýPort cílováIP cílovýPort názevAplikace". Tuto funkci jsem částečně převzal z internetu[3].

4 Použití aplikace

Parametry programu jsou následující:
Argument ***-s*** specifikuje IP adresu syslog serveru, na který budou odesílány zprávy.
Argument ***-i*** specifikuje časový interval, po jehož uplynutí se znovu kontroluje seznam spojení.
Argument ***-f*** specifikuje filtr aplikací, které budou kontrolovány.
Všechny výše uvedené argumenty jsou povinné. Argumenty mohou být zadávány libovolně.

5 Metriky kódu

Počet souborů: 1 soubor
Počet řádků zdrojového kódu: 440 řádků
Velikost spustitelného souboru: 40 325B

6 Reference

[1] https://cs.wikipedia.org/wiki/NetFlow
[2] http://www.wikiwand.com/cs/Lsof
[3] http://tinyurl.com/84x2ya3