Posudek oponenta bakalářské práce

Student: Nahálka Roman
Téma: Extrakce tunelovaných dat do samostatných toků (id 20798)
Oponent: Hranický Radek, Ing., UIFS FIT VUT

1. Náročnost zadání **méně obtížné zadání**

Zadání považuji za méně obtížné, jelikož problém samotný není nijak komplexní a velkou část práce za studenta řeší program TShark.

2. Splnění požadavků zadání **zadání splněno**

3. Rozsah technické zprávy **je v obvyklém rozmezí**

Technická zpráva čítá 34 stran vysázených v LaTeXu, je tedy v obvyklém rozsahu.

4. Prezentační úroveň předložené práce **85 b. (B)**

Práce má logickou strukturu a jednotlivé kapitoly na sebe navazují. Autor uvádí pouze informace relevantní k tématu a to na rozumné úrovni abstrakce.

5. Formální úprava technické zprávy **90 b. (A)**

Po stránce typografické a jazykové je technická zpráva na velmi dobré úrovni. Text práce je čtivý a srozumitelný. Jen občas se vyskytují drobné nedostatky, např. anglický slovosled: "PCAP soubory", apod. Pozitivně též hodnotím srozumitelná schémata a diagramy.

6. Práce s literaturou **55 b. (E)**

Autor používá relevantní prameny vzhledem k tématu, jejich použití je však na pováženou. V práci dochází k mísení dvou citačních stylů. V kapitole 2 není jasné, které pasáže čerpají ze dvou zmíněných knih a které z dokumentů RFC. V kapitole 3 autor problém citování pramenů řeší prohlášením, že informace byly volně převzaty z knihy Practical Packet Analysis. Tento způsob řešení nepovažuji za šťastný. U použitých nástrojů by neškodila poznámka pod čarou s odkazem na web.

7. Realizační výstup **65 b. (D)**

Realizační výstup je rozsahem poměrně skromný a představuje 866 řádků v jazyce Python 3. Nástroj je schopen detekovat několik typů tunelovaného provozu a z tohoto provozu následně odstranit hlavičky tunelovacích protokolů. Volitelně je možné též provoz rozdělit do více souborů dle síťových toků v souboru původním. Toto splňuje zadání, ovšem řešený problém je poměrně triviální. V komentářích je použita diakritika, avšak jen na některých místech.

8. Využitelnost výsledků

Realizační výstup může nalézt využití jako doprovodná součást jiného nástroje. Práce však staví jen na existujících poznatcích a v oblasti zpracování síťových dat nepřináší nic nového, ani nedemonstruje nějaké zajímavější postupy.

9. Otázky k obhajobě

1. Jaké úpravy by bylo nutné provést, aby aplikace podporovala extrakci šifrovaného provozu? Předpokládejte, že šifrovací klíče máte k dispozici.
2. Jaké úpravy by bylo potřeba provést, aby aplikace mohla pracovat i s provozem zachytávaným v reálném čase?

10. Souhrnné hodnocení **70 b. dobře (C)**

Zadání bylo splněno, ovšem řešený problém je poměrně triviální. Práce neprezentuje něčím inovativní principy ani komplexnější postupy. Technická zpráva, až na práci s literaturou, je však zpracována kvalitně a působí velice dobrým dojmem. Praktickým experimentům ovšem mohlo být věnováno více prostoru. Práci hodnotím jako slabší C.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 31. května 2018

.....

podpis