Posudek oponenta bakalářské práce

Student: Hmeľár Jozef, Bc.
Téma: Analýza zachyceného DNS provozu (id 15142)
Oponent: Kekely Lukáš, Ing., UPSY FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Dle mého názoru se jedná o průměrně obtížné zadání, které si student sám nijak nerozšířil.

2. Splnění požadavků zadání **zadání splněno s drobnými výhradami**

Ne úplně splněny jsou podle mě tyto body zadání:

- 3) Popis analýzy na určení použitelných sledovaných položek a statistických ukazatelů DNS mi nepřijde dostatečně podrobný resp. dostatečně podrobně popsán v textu práce.
- 4) Přehlednost výstupů implementovaného nástroje a popisu jeho ovládání by mohla být místy i trochu lepší.
- 6) Zhodnocení výsledků by mohlo být podrobnější a více průkazně zpracováno.

Nejedná se ale o závažné nedostatky, jen drobné nedokonalosti.

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

Rozsah technické zprávy je v obvyklém rozmezí.

4. Prezentační úroveň předložené práce **55 b. (E)**

Text práce místy postrádá zjevnou návaznost a některé jeho části působí zbytečně z pohledu zaměření práce nebo informačního přínosu (například sekce 2.8). Na druhé straně, jsou ale jiné zajímavější části textu sepsány příliš povrchně a neposkytují čtenáři dostatečně podrobnou informaci. Například sekce 2.4 popisuje přenos zónový souborů v DNS, ale v práci zcela chybí popis co to DNS zóna je; nebo kapitola 4 neobsahuje popis detailů použitého způsobu zpracování jednotlivých paketů a rozpoznání protokolu DNS v nich, popis jádra implementace (sekce 4.1) jen jinými slovy přepisuje text jednoduchého návrhu kostry aplikace (sekce 3.3).

Dalším objeveným nedostatkem je chybějící popis obrázků v celém textu práce. Na ty se autor v textu jenom odkazuje bez bližšího popisu co je na nich zobrazeno/zajímavého. Výrazným příkladem je obrázek 2.5 zobrazující iterativní DNS dotaz, který je uveden a popsán jen větou "Na obrázku 2.5 môžeme vidieť, ako táto iteratívna žiadosť vyzerá.". Přitom, popisu druhého typu DNS dotazu (obrázek 2.4) je věnována půlka strany.

Dále, zhodnocení výsledků v kapitole 5 není dostatečně průkazné a informativní pro čtenáře. Časová a paměťová náročnost jsou uváděny v sekundách a bajtech při zpracování konkrétních souborů. Chybí ale popis velikosti a charakteru dat v těchto souborech. Zcela zbytečně působí i graf na obrázku 5.1.

Kvůli uvedeným nedostatkům, text práce celkově působí jako sepsán ve spěchu resp. na poslední chvíli.

5. Formální úprava technické zprávy **55 b. (E)**

Práce trpí několika formálními nedostatky:

- v celém textu jsou časté překlepy či gramaticky nesprávné formulace, přítomny jsou dokonce již v abstraktu či úvodu
- jednoznakové předložky na koncích řádků
- nekonzistentnost citací, některé odkazy jsou uvedeny v poznámkách pod čarou (napr. strana 4)
- používání rastrových obrázků, někdy s použitím nedostatečné velikosti písma nebo celkového rozlišení
- nejednotnost v stylu kreslení obrázků, každý obrázek je nakreslen jinak, co je nejzjevnější u obrázků 2.4 a 2.5 ilustrujících dvě podobné věci
- anglické popisky u většiny obrázků
- použití několika anglických termínů v textu, i když k nim existujícími české ekvivalenty (například "bezznamienkový šestnásť bitový integer", parsovať, packet)

- popisky grafů psány verzálkami a bez diakritiky

Text práce tak celkově působí napsán neodborně nebo ve spěchu bez zpětné kontroly.

6. Práce s literaturou **65 b. (D)**

Student používá zdroje uvedené v zadání i samostatně nalezené. Některé z nich však nejsou primární, ale jde pouze o webové stránky popisující základy dané problematiky (například [15-17]).

7. Realizační výstup **65 b. (D)**

Student implementoval funkčně poměrně kvalitní program na analýzu DNS dát. Program je schopen zpracovat soubory obsahující celé pakety (PCAP formát) i záznamy o tocích (CSV nebo NetFlow formát). Nedostatkem je, ale slabší intuitivnost ovládaní způsobená nedostatečnou dokumentací a též neúplné ošetření chybně zadaných vstupů.

8. Využitelnost výsledků

Výslednou implementaci je možno prakticky využít k získání dodatečných informací o zachycených DNS útocích. Získané informace je pak možno využít k zlepšení obrany proti budoucím útokům na DNS.

9. Otázky k obhajobě

- V kapitole 4 schází podrobný popis implementace zpracování jednotlivých paketů. Zajímalo by mě tedy, jak je to ve Vaší implementaci realizováno? Zejména pak, jak jsou pakety analyzovány, které protokoly nižších vrstev jsou podporovány (VLAN, MPLS, IPv4, IPv6, …) a jak jsou rozpoznány pakety obsahující DNS?

- Výkonnost programu je v kapitole 5 uváděna jen jako doba běhu při zpracování konkrétních souborů, co není příliš vypovídající. Jaká je tedy výkonnost programu v jednotlivých testech z kapitoly 5 zapsaná v počtu zpracovaných záznamů (paketů) za sekundu? Je podle Vás dosažena výkonnost dostatečná nebo je možno/potřeba zpracování zefektivnit?

- Je možno zpracování velkých souborů s DNS daty a výpočet jednotlivých statistik nad nimi jednoduše paralelizovat? V čem vidíte případné problémy omezující výkonnost nebo realizovatelnost takovéto více-vláknové implementace analýzy DNS?

10. Souhrnné hodnocení **58 b. dostatečně (E)**

Student sice v rámci bakalářské práce vytvořil použitelný program pro analýzu DNS, ale text samotné práce ani popis ovládání programu nejsou velice kvalitní. Početné nedostatky v textu práce jsou podrobně rozebrány v jednotlivých sekcích hodnocení. Celkově práce a její výsledky budí dojem vypracování ve spěchu (na poslední chvíli) a bez zpětné kontroly. Navrhuji proto výslední hodnocení E.

V Brně dne: 5. června 2015

.....
podpis