Posudek oponenta diplomové práce

Student: Krůl Michal, Bc.
Téma: Korelace IPFIX záznamů z provozu proxy serverů (id 25281)
Oponent: Jeřábek Kamil, Ing., UIFS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Zadání hodnotím jako průměrně obtížné.

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

Zadání bylo splněno. Jsou zde však drobné výhrady k testování, kde se objevují ne vždy úplně jasné výsledky.

3. Rozsah technické zprávy **splňuje pouze minimální požadavky**

Práce se pohybuje blízko spodní hranice obvyklého rozmezí diplomové práce.

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

Práce je logicky strukturovaná, členěná do kapitol, které na sebe vzájemně navazují. Práce je místy hůře čitelná vzhledem k opakování lehce přeformulovaných bloků textu viz například strana 21.

Část práce zabývající se testováním obsahuje ne vždy jasné prezentované výsledky.

Nicméně je zde vidět zlepšení a částečné přestrukturování textu, které vede k lepší logické návaznosti.

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

Práce obsahuje typografické nedostatky, opakující se slova či překlepy. Občas se vyskytující hovorové výrazy, zejména v závěrečné části práce.

V prohlášení je uvedena bakalářská práce, i přesto, že se jedná o diplomovou práci.

6. Práce s literaturou **59 b. (E)**

Student se v práci odkazuje na relevantní zdroje z oblasti řešeného problému. Na některých místech se však jeví, že citace chybí. Zároveň není vždy z umístění citace v textu jednoznačně jasné, co konkrétně je přejato.

7. Realizační výstup **50 b. (E)**

Práce se teoreticky věnuje různým typům proxy serverů, primárně forwarding (v práci uváděno jako dopředné), zřetězené a reverzní proxy. Řešením omezuje pouze na forwarding proxy (HTTP, HTTPS) formou mapování hodnot primárně aplikačních protokolů získaných sondou společnosti Flowmon a jakousi manuálně nastavenou "časovou heuristikou" (v práci uváděno časová korelace).

V rámci práce student vytvořil datovou sadu obsahující vytvořený zachycený provoz, který následně využívá pro analýzu, návrh a testování výsledného řešení.

Řešení sestává z programu v jazyce Python, načítajícím csv soubor na vstupu a vytvářejícím csv soubor s mapováním identifikátorů nalezených korelovaných toků.

Vytvořený program je spustitelný a jeví se alespoň jako funkční.

Validační a verifikační část je již možné hodnotit jako dostatečnou, avšak její kvalitu snižuje ne vždy jasný popis obsahu testů (zdali se testují HTTP či HTTPS korelace, nebo obojí zároveň). Jak a z čeho byla vypočítána úspěšnost, obsahuje alespoň hodnoty, a je tedy možné se hodnot dopátrat.

8. Využitelnost výsledků

Výsledný program by mohl být využit v rámci firmy Flowmon.

9. Otázky k obhajobě

1. V tabulce 7.2 se jedná o pouze HTTP, či HTTPS, či mixované toky, případně v jakém poměru?
2. Jak byly získány hodnoty ve sloupci "Nalezené korelace (korelované záznamy)" v tabulce 7.3?
3. Čím si vykládáte tak nízkou úspěšnost u záznamů "win+linux" a "zřetězené (2 soubory)" v tabulce 7.3?
4. Proč pro HTTP korelace nepoužíváte další extrahované informace jako jsou HTTP_REQUEST_URL, HTTP_REQUEST_URL_SHORT, HTTP_REQUEST_AGENT, HTTP_RESPONSE_STATUS_CODE,

a další?

10. Souhrnné hodnocení

54 b. dostatečně (E)

Diplomová práce se zaměřuje na korelaci IPFIX záznamů toků, získaných Flowmon sondou, před, za a mezi proxy servery. Student nastudoval a seznámil se s principy proxy serverů a technologii NetFlow/IPFIX. Práce se však omezuje pouze na forwarding proxy servery a protokoly HTTP a HTTPS a mapování hodnot extrahovaných z toků, čímž se práce velmi značně zjednodušuje. V rámci práce student nastavil virtuální prostředí, v němž vytvořil datovou sadu skládající se ze zachyceného síťového provozu, kterou následně používá pro analýzu, návrh a testování výsledného řešení.

Textová část se blíží dolní hranici obvyklého rozmezí. V textové části se opakují bloky textu a místy je velmi těžce pochopitelná. Část testování a validace není vždy úplně jednoznačná, avšak již se dá považovat za dostatečnou.

U práce je jednoznačně vidět její dostatečné vylepšení, nicméně jsou zde stále některé zmíněné nedostatky. Navrhuji E jako výsledné hodnocení.

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

V Brně dne: 2. srpna 2022

Jeřábek Kamil, Ing.
oponent