Review of Bachelor's Thesis

Student: Uhříček Daniel
Title: Multiplatform Linux Sandbox for Analyzing IoT Malware (id 22120)
Reviewer: Burget Radek, Ing., Ph.D., UIFS FIT VUT

1. Assignment complexity — **more demanding assignment**

Zadání vyžadovalo studium a zvládnutí souvisejících technologií v širokém spektru oblastí, které zahrnuje analýzu malware, operační systémy, síťové protokoly a další. Zadání proto hodnotím jako obtížnější.

2. Completeness of assignment requirements — **assignment fulfilled**

Zadání považuji za splněné. Bodu 5 (testování na vzorcích malware) není věnováno mnoho prostoru, bylo však evidentně provedeno. Naopak z hlediska rozsahu implementovaných nástrojů bylo zadání výrazně rozšířeno, jak uvádím níže.

3. Length of technical report — **in usual extent**

Rozsah technické zprávy je v rozmezí obvyklém pro bakalářskou práci.

4. Presentation level of technical report — **78 p. (C)**

Technická zpráva obsahuje pěkně zpracovanou část věnovanou analýze malware obecně, souvisejícím technologiím a nástrojům. Část věnovaná návrhu, implementaci a testování vlastního řešení je poněkud stručnější a plně neodráží objem práce, který student odvedl na vytvořeném řešení. Ačkoliv všechny detaily jsou na různých místech technické zprávy popsány, postrádám zejména jasné shrnutí toho, které komponenty student vytvořil sám, jaké integroval nástroje třetích stran a jaký je předpokládaný scénář nasazení.

5. Formal aspects of technical report — **84 p. (B)**

Technická zpráva je psána v angličtině na velmi dobré úrovni, pouze ojediněle lze narazit na zvláštní slovní spojení a zcela výjimečně na drobné chyby. Po typografické stránce je práce rovněž pečlivě zpracována.

6. Literature usage — **94 p. (A)**

Seznam použité literatury je značně rozsáhlý a obsahuje relevantní zdroje, které jsou v textu práce řádně citovány.

7. Implementation results — **98 p. (A)**

Realizační výstup je velmi rozsáhlý a kromě vlastního virtuální prostředí pro spouštění malware obsahuje mnoho dalších komponent. Jedná se např. o nástroje pro analýzu síťové kominukace, infrastrukturu automatizující použití virtuálního prostředí a v neposlední řadě pěkně navrženou infrastrukturu pro spouštění úloh založenou na webových technologiích a mikroslužbách. V tomto bodě student podle mého názoru výrazně rozšířil původní zadání.

8. Utilizability of results

Vytvořené nástroje jsou k dispozici jako software s otevřeným kódem a jsou plně použitelné v praxi, o čemž svědčí i zpětná vazba viditelná např. na serveru GitHub u příslušných projektů.

9. Questions for defence

1. Bylo by možné vytvořený systém nasadit i v distribuovaném prostředí, tzn. pro analýzu malware paralelně na více výpočetních uzlech?

10. Total assessment — **92 p. excellent (A)**

Pan Uhříček v rámci své bakalářské práce navrhl a implementoval větší množství nástrojů, které spojil do komplexního celku. Výsledné řešení je rozsáhlé, plně funkční a použitelné v praxi. K technické zprávě lze mít různé drobné připomínky, kvalita, rozsah a praktická použitelnost výsledného softwarového díla však podle mého názoru převažují a navrhuji proto hodnocení stupněm A.

In Brno 27. May 2019

.....
signature