Posudek oponenta bakalářské práce

Student: Ďuriš Tomáš
Téma: Automatizace nasazení a sběru dat z honeypotů (id 23239)
Oponent: Pluskal Jan, Ing., UIFS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Práce si klade za cíl automatizovat nasazení zvolených honeypot na servery pod správou uživatele přístupné skrz SSH. Práce je spíše konfigurační povahy využívající existující nástroje a služby. Nicméně úspěšné splnění zadání vyžadovalo nastudovat aktuálně používané technologie pro nasazení, monitorování a vybrat vhodné kandidáty.

2. Splnění požadavků zadání **zadání splněno**

Práce obsahuje nejen otestování v reálném provozu, ale taktéž částečnou analýzu zaznamenaných výsledků.

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

4. Prezentační úroveň předložené práce **90 b. (A)**

Jednotlivé kapitoly na sebe logicky navazují a práce je pro čtenáře obecně pochopitelná. Nicméně najdou se úseky, kde bez znalosti interní terminologie firmy Avast není význam naprosto zřejmý - "Dracula server" viz obr. 4.1.

5. Formální úprava technické zprávy **75 b. (C)**

Práce je ve slovenském jazyce, nemohu plně hodnotit gramatiku. Nicméně práce obsahuje řadu překlepů a gramatických chyb.

- chybějící tečky na konci vět, nekonzistentní výčty - str. 4
- překlepy - sekce 2.1 ", aby aby", nadpis kapitoly 6 "anlýza"
- neuvedení typu reference - sekce 3.3 obsahuje "(viz 3.3)"
- nekonzistentní rozdělovníky - 4.4
- nekonzistentní kapitalizace - obr. 5.5

6. Práce s literaturou **85 b. (B)**

Literatura obsahuje relevantní prameny. U pramenů 5, 16 není zřejmé, o jaký zdroj se jedná.

7. Realizační výstup **95 b. (A)**

Realizační výstup tvoří sada konfiguračních souborů a skriptů nasazující vybrané honeypoty. Oceňuji, že je zde podpora pro výběr verze, migraci konfigurace a obnovení předchozí verze v případě, že nasazení selže. Licence zdrojových souborů není explicitně přiložena, nicméně použité technologie obsahují open source licence.

Autor upravil konfigurace honeypot nad rámec zadání, aby zmezil její triviální identifikaci.

8. Využitelnost výsledků

Práce je kompilačního charakteru. Programový výstup práce je prakticky použitelný v produkčním nasazení firmy Avast.

9. Otázky k obhajobě

1. Jak je zamýšlena práce s testovacím Docker nasazením? V rámci Dockerfile využíváte vždy "latest" verze. Jak je zajištěna konzistence s nasazovanými verzemi, které při nasazení získáte ze zdrojových kódů.

10. Souhrnné hodnocení **85 b. velmi dobře (B)**

Práce i přes svůj převážně konfigurační charakter vykazuje logický přístup k řešení problému automatizovaného nasazení honeypot serverů. Výsledek práce bude dále využíván společností Avast v produkci. I přes drobné nedostatky v formální úpravě, navrhuji práci hodnotit stupněm B jako velmi dobrou.

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

V Brně dne: 2. června 2021

Pluskal Jan, Ing.
oponent