Hodnocení vedoucího bakalářské práce

Student: Kučma Tomáš
Téma: Systém pro automatický sběr, vyhodnocení a aktualizaci YARA pravidel (id 25023)
Vedoucí: Regéciová Dominika, Ing., UIFS FIT VUT

1. **Informace k zadání**
   Bakalářskou práci hodnotím jako obtížnější. Bylo potřeba se podrobně seznámit s komplexními nástroji pro detekci škodlivých souborů, a zároveň vlastností jazyka YARA, aby na ně mohl student navazovat v podobě nástrojů pro sběr, vyhodnocování kvality a aktualizaci pravidel. Student splnil všechny body zadání.
2. **Práce s literaturou**
   Student si hledal zdroje informací aktivně sám. Čerpal především z technických dokumentací a vzhledem k povaze zadání považuji tento seznam za dostatečný.
3. **Aktivita během řešení, konzultace, komunikace**
   Student sice aktivně pracoval na zadání spíše až v průběhu letního semestru, pravidelně však konzultoval práci, jak se mnou, tak konzultantem. Na konzultace chodil připraven.
4. **Aktivita při dokončování**
   Při dokončování byla práce mírně zvýšená, převážně kvůli analyzování výsledků implementace a analýze kvality YARA pravidel z vybraných zdrojů. Práce však byla dokončena včas a konzultována v předstihu.
5. **Publikační činnost, ocenění**

6. **Souhrnné hodnocení** **velmi dobře (B)**
   Studen nastudoval nástroje pro detekci škodlivého malwaru ve firmě Avast se zaměření hlavně na nástroj YARA a vlastnosti jeho jazyka. Student poté navrhl a implementoval systém pro sběr, vyhodnocení a aktualizaci YARA pravidel z vybraných zdrojů. Vše zároveň pečlivě otestoval, kód prošel kontrolou od konzultanta a student vše na závěr zhodnotil.
   Systém byl nasazen a je používán při detekci škodlivého softwaru firmou Avast.
   Z těchto důvodů navrhuji hodnocení za B.

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

V Brně dne: 17. května 2022

Regéciová Dominika, Ing.
vedoucí práce