Posudek práce

předložené na Přírodovědecké fakultě JU

❑posudek vedoucího ☑posudek oponenta
☑ bakalářské práce ❑ diplomové práce

Autor/~~ka~~: Jan Soubusta
Název práce: Vizualizace síťového provozu s ohledem na bezpečnostní události
Studijní program a obor: Aplikovaná informatika
Rok odevzdání: 2020

Jméno a tituly ~~vedoucího~~/oponenta: Mgr. Michal Konopa
Pracoviště: UAI PRF JU
Kontaktní e-mail: konopm05@prf.jcu.cz

Odborná úroveň práce:
❑ vynikající ☑ velmi dobrá ❑ průměrná ❑ podprůměrná ❑ nevyhovující

Věcné chyby:
❑ téměř žádné ☑ vzhledem k rozsahu přiměřený počet ❑ méně podstatné četné ❑ závažné

Výsledky:
❑originální ❑ původní i převzaté ☑ netriviální kompilace ❑ citované z literatury ❑ opsané

Rozsah práce:
❑ veliký ☑ standardní ❑ dostatečný ❑ nedostatečný

Grafická, jazyková a formální úroveň:
❑ vynikající ☑ velmi dobrá ❑ průměrná ❑ podprůměrná ❑ nevyhovující

Tiskové chyby:
☑ téměř žádné ❑vzhledem k rozsahu a tématu přiměřený počet ❑ četné

Celková úroveň práce:
❑ vynikající ☑ velmi dobrá ❑ průměrná ❑ podprůměrná ❑ nevyhovující

Slovní vyjádření, komentáře a připomínky ~~vedoucího~~/oponenta:

Grafická, jazyková a formální úroveň:

- velmi dobrá pravopisná úroveň, občas chyby ve složitějších souvětích
- autor někdy volí podivná slovní vyjádření (např. „těžká složitost“)
- obrázky by mohly být čitelnější – zvláště u grafů
- opakující se zdroje v seznamu použité literatury, např. odkaz na Bartelovu diplomovou práci je zde uveden 4 krát pod různými čísly

Odborná úroveň:

- Text práce se snadno čte, je přehledný, týká se dané problematiky. Některé popisy jsou nadbytečné – např. detailní popis práce s Grafanou, který lze v případě potřeby snadno najít v dokumentaci.
- Očekával bych, že autor vyvine větší úsilí při sběru metrik, které nejsou přímo podporovány jím zvolenými softwarovými nástroji. Týká se to např. sběru dat produkovaných nástrojem scanlogd. Nástroje, které umožňují sbírat tato data, je možné prostřednictvím pluginů integrovat s řešením, které použil autor. Místo toho se v podstatě omezuje na konstatování, že chybí přímá podpora.
- Práce měla rozhodně do větší míry probrat různé možnosti zobrazení jednotlivých metrik včetně jejich kombinací (které mohou poskytnout lepší celkový přehled situace). Místo toho se omezuje na 2D-grafy, kde osa X stabilně reprezentuje čas a osa Y danou metriku, což není pro analýzu některých síťových anomálií (například skenování portů) vždy to nejvhodnější řešení.

Celková úroveň práce je i přes uvedené připomínky velmi dobrá. Uvedené typy síťových útoků jsou zvoleny rozumně, popis řešení je vzhledem k cílům práce snadno srozumitelný a kompletní.

Případné otázky při obhajobě a náměty do diskuze:

Práci
☑ doporučuji
❑ nedoporučuji
uznat jako ~~diplomovou~~/bakalářskou.

Navrhuji hodnocení stupněm:
❑ výborně ☑ velmi dobře ❑ dobře ❑ neprospěl/a

Místo, datum a podpis vedoucího/oponenta:
V Českých Budějovicích 29. 06. 2020