Posudek práce

předložené na Přírodovědecké fakultě JU

☐ posudek vedoucího ☑ posudek oponenta
☐ bakalářské práce ☑ diplomové práce

Autor/ka:	**Bc. Tomáš Starý**
Název práce:	**Výzkum a implementace open-source řešení IDS/IPS systému jako ochranu proti aktuálně probíhajícím hrozbám v prostředí velkého poskytovatele internetových služeb**
Studijní program a obor:	Aplikovaná informatika
Rok odevzdání:	2020

Jméno a tituly vedoucího/oponenta:	Ing. Marta Vohnoutová
Pracoviště:	Ústav aplikované informatiky
Kontaktní e-mail:	mvohnoutova@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:

Práce si klade za cíl nasazení open-source řešení IDS/IPS systému prostřednictvím platformy Docker.
Na práci jsem byla velmi zvědavá a začala jsem ji číst s velkým očekáváním. V první polovině práce jsem se dozvěděla, co je Docker a co je IPS a IDS na úrovni Wikipedie nebo nižší. V druhé části ve stejném duchu povšechný popis open-source kandidátů na nasazení. Jejich vlastní porovnání srovnávaných open-source IDS/IPS systémů bylo nedostatečné, vlastně celý výběr rozhodla podpora multi-threadingu. Po dalším čtení na Internetu nicméně musím s autorovým výběrem Suricata souhlasit. Dále následovala neučesaná kopa informací o nasazení a testování. Marně jsem hledala nějaké konkrétnější obrázky, síťové zapojení, schémata, tabulky a informace se musí pracně vyzobávat z textu. Text byl vlastně takové „neučesané" povídání, ze kterého plynulo, že autor něco vytvořil.
Text někde obsahoval množství nezajímavých věcí, zatímco konkrétní informace autor obešel – např. „Bylo nutné použít některá stará pravidla……"
V textu jsem se ztrácela. Podle mého názoru daná práce svou kvalitou velmi obtížně splňuje požadavky na magisterskou práci a vlastně autor neumí prodat, co při nasazování a konfiguraci systému Suricata odpracoval.

Případné otázky při obhajobě a náměty do diskuze:

1. Popište stará pravidla a řekněte, která z těchto starých pravidel se musela ponechat, která zanikla, která byla modifikována a nebo nahrazena jinými.
2. Uvádíte tvorbu logů a jejich zpracování nějakým SIEM nástrojem. Popište, jak probíhá tvorba logů a jejich shromažďování na SIEM (např."generování alertu do souboru s logy"). Co loguje Vámi nastavená Suricata? Je nějaká reakce na logy ze Suricaty?

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 dne 14. ledna 2020

.....