Posudek práce

předložené na Přírodovědecké fakultě JU

☐ posudek vedoucího ☒ posudek oponenta
☐ bakalářské práce ☒ diplomové práce

Autor/ka: Bc. Jaroslav Kovář
Název práce: Analýza škodlivého kódu ve virtuálním prostředí
Studijní program a obor: Aplikovaná informatika
Rok odevzdání: 2019

Jméno a tituly ~~vedoucího~~/oponenta: Marek Anýž
Pracoviště: CETIN, správa antivirového řešení
Kontaktní e-mail: marek.anyz@cetin.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 jako celek je napsána přirozeně a přehledně. Zabývá se tématem a jeho možnostmi do budoucna důležitými při obraně soukromí a informací. Dané téma zdaleka přesahuje časové možnosti diplomové práce, nicméně se autorovi povedlo velmi pěkně připravit základ pro jeho případný další výzkum v této oblasti. Musím ocenit nápad použití VDI a použití flash disku jako primárního media a s tím využití výhod tohoto řešení a použití různých analytických nástrojů vedoucí k přesnější detekci.

Případné otázky při obhajobě a náměty do diskuze:
Domníváte se, že v blízké budoucnosti je možné a ekonomicky výhodné použití strojového učení v analýzách škodlivého kódu ve VDI/sandboxu oproti manuální analýze? Případně proč se tak domníváte.
V analýze jste jako HW počítač použil OS Windows 10 64b, ale na virtuálním prostředím jste použil stroje s OS Windows 7 64b. Jaké rozdíly v detekci a případnému chování škodlivého kódu byste očekával v různých verzích OS Windows? Doporučil byste případně kombinaci verzí OS Windows v rámci virtuálních prostředí, jako více stupňové analytické prostředí a proč?

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

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

Místo, datum a podpis ~~vedoucího~~/oponenta:
V Praze dne 8.1.2020