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:	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 vytvoření prostředí pro analýzu škodlivého kódu ve virtuálním prostředí. Zaměření je především proto evasivnímu malware.

Začnu výtkou, v úvodních částech práce (pravděpodobně překládaných) je tak strašlivá čeština, že jsem musela některé věty číst vícekrát, abych je pochopila. Ale jakmile se autor dostal k vlastnímu vyjadřování, tento problém šílené češtiny naštěstí zmizel. Některé popisy v úvodu práce budí dojem, že byly vkládány do textu, aby „zaplácly" obsah korespondující s názvem kapitoly. Text by mohl být také přehlednější – forma tabulek, odrážek, obrázků apod., oddělovat jasně opatření prováděná autorem práce od vlastností SW a úprav nasazeného SW, obtížně jsem to rozlišovala. Potud výtky.

Autor předkládá práci, která je velmi zajímavá, v místech, kde používá autor vlastní jazyk, je i velmi čtivá. Téma analogie chování počítačových virů s živými viry je velmi aktuální.
Autor vytvořil virtuální prostředí s několika stroji a simulovanou virtuální sítí, které postupně maskoval na různou úroveň maskování jak celého virtuálního prostředí, tak jednotlivých souborů a aplikací a porovnával úspěšnost při nasazování chytrého malwaru, který se umí chovat podle toho, jaké prostředí a aplikace detekuje. Popisuje a zdůvodňuje výběr aplikací a operačních systémů. Dále popisuje funkce jednotlivých strojů ve virtuálním prostředí a pracovní postupy při nasazování evasivního malware.

Celkový dojem z práce je přes úvodní výtky velmi dobrý a je z ní patrno, jak mnoho toho autor odpracoval. Práce obsahuje mnoho podrobných údajů a postřehů z chování evasivního malware, který jeho řešením „dostal adekvátního protivníka".

Případné otázky při obhajobě a náměty do diskuze:

1. Na obr. 13 je poněkud nepřehledný obrázek – virtualizovaný výstup nástroje ProcDOT, popište jej srozumitelněji než je v textu práce
2. Není mi úplně jasné, jaké procesy jsou automatické a jaké jsou prováděny obsluhou ručně. Popište stupeň automatizace vašeho řešení a možnosti další automatizace, případně možnosti dalšího rozvoje Vašeho řešení.
3. Nekonzultoval jste vaše řešení s některým tvůrcem antivirů ?

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