FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Simona Fornůsek, Ph.D.
Student:	Bc. Martin Mandík
Název práce:	Techniky perzistence malware a její detekce
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	1. června 2024

Hodnotící kritéria

1. Splnění zadání

▸ [1] **zadání splněno**
[2] zadání splněno s menšími výhradami
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Všechny body zadání byly bez výhrad splněny.

2. Písemná část práce 90 / 100 (A)

Písemná část práce je detailní a dobře strukturovaná. Student pečlivě rozebral techniky perzistence, související artefakty, a i možnosti detekce. Oceňuji i rešerši technik, které dnes malware využívá - na této rešerši student postavil výběr technik pro tvorbu detekcí, čímž maximalizuje potenciál praktického využití.

3. Nepísemná část, přílohy 95 / 100 (A)

V rámci nepísemné části práce student přikládá konfigurační soubory prostředí, i veškeré zpracované detekční pravidla - dohromady s kapitolami 3 a 4 tak umožňuje snadnou replikaci navržených detekcí.

4. Hodnocení výsledků, jejich využitelnost 90 / 100 (A)

Téma práce je velmi aktuální, a vzhledem ke kvalitní rešerši, a i vypracovaným detekčním pravidlům má praktické uplatnění. Rovněž zvolené nástroje pro implementaci jsou aktuální a dnes široce využívané, což ještě zvyšuje praktickou využitelnost.

5. Aktivita studenta

▸ [1] **výborná aktivita**

[2] velmi dobrá aktivita
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Student byl velmi aktivní, práci se pečlivě věnoval, pravidelně přicházel na konzultace s vlastními nápady, a byl dobře připravený.

6. Samostatnost studenta

▸ [1] **výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Celkové hodnocení 95 /100 (A)

Vzhledem ke kvalitnímu zpracování tématu práci doporučuji k obhajobě.

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.