FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Simona Fornůsek, Ph.D.
Student:	Bc. Silvie Němcová
Název práce:	Analýza technik "Lateral movement" v systémech s OS Windows
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

Ze čtyř bodů zadání je většina práce věnována prvním dvěma bodům. Body 3 a 4 ze zadání, které měly být praktičtější a implementační částí práce, jsou nakonec pokryty v kapitole 6 pouze pro jednu techniku "Replication through removable media", nutno ale říci, že tuto techniku studentka rozpracovala vcelku do detailu. Pro obecnější detekci laterálního pohybu by však bylo nutné pokrýt technik víc.
Do jisté míry je to způsobeno tím, že se studentka soustředila, a příliš mnoho času strávila nad teoretickou částí, a poté technickými problémy, na které narazila během přípravy testovacího prostředí, a na další části ji tak už zbylo méně času.

2. Písemná část práce 70 / 100 (C)

Písemná část práce, co se týče teoretického úvodu, přístupu k tvorbě pravidel i rešerše existujících možností detekce je obšírná a detailní, studentka nastudovala mnoho materiálů a zdrojů.
Jak již ale bylo zmíněno v prvním bodě, chybí detailnější rozebrání dalších technik laterálního pohybu.

3. Nepísemná část, přílohy 50 / 100 (E)

Implementované detekce jsou v pořádku, nicméně, pro obecnější detekci laterálního pohybu by bylo nutné pokrýt technik víc.

4. Hodnocení výsledků, jejich využitelnost 50 /100 (E)

Pro plné uplatnění a praktické využití, by práce musela být dotažená, a kapitola 6 rozšířena o rozbor a implementaci dalších technik laterálního pohybu. V aktuálním stavu může posloužit pro čtenáře jako teoretický úvod do tvorby detekcí, v kapitole 5 studentka zpracovala systematický přístup k přípravě detekcí, který lze zajisté využít, a nakonec detekce z kapitoly 6 může posloužit jako modelový příklad pro další rozšíření.

5. Aktivita studenta

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

Studentka byla během psaní práce aktivní a pečlivá, pravidelně konzultovala a přicházela s vlastními nápady. Přípravě práce věnovala hodně času, bohužel, jak jsem zmiňovala v prvním bodě, čas na jednotlivé body zadání si nerozložila nejefektivněji.

6. Samostatnost studenta

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

Celkové hodnocení 60 /100 (D)

I přes výtky k splnění zadání, bych práci doporučila k obhajobě - a to zejména z důvodu široké teoretické části, množství zdrojů které studentka zpracovala, a jejímu systematickému přístupu.

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.