FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	prof. Ing. Róbert Lórencz, CSc.
Student:	Bc. Stanislav Lepič
Název práce:	Detekční Pravidla pro Detekci Ransomware ve Formátech YARA a Sigma
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	3. 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

Práce vykazuje nedostatky tykající se systematičtějšího přístupu a to jednak v rešeršní - úvodní částí práce, tak i v kapitolách popisující řešení úloh vyjmenovaných v zadání práce.

2. Písemná část práce 64 /100 (D)

Struktura práce je logická, nicméně, jednotlivé kapitoly by si zasloužily hlubší zpracování. V současné podobě je problematika pojata spíše povrchně, bylo by užitečné přidat podrobnější popis chování ransomware, aby práce působila přesvědčivěji.
Rovněž v práci nejsou prakticky popsány výsledky testování, závěry jsou strohé a nepodložené daty.

3. Nepísemná část, přílohy 69 /100 (D)

V rámci příloh student přikládá vytvořená pravidla. Chybí popis konfigurace prostředí, testovací skripty, výsledky testování.

4. Hodnocení výsledků, jejich využitelnost 67 /100 (D)

Detekce v rámci této práce jsou zaměřeny pouze na omezený rozsah chování zkoumaných vzorků, což značně omezí jejich praktické využití. Při širším praktickém nasazení by bylo nezbytné rozpracovat detekční metody do většího detailu a zahrnout širší spektrum chování ransomware.

Praktické využití v reálných scénářích by vyžadovalo, aby detekce pokrývala široké spektrum chování ransomware, včetně různých variant a technik.

Celkové hodnocení

64 /100 (D)

Práce formálně obsahuje řešení všech bodů zadání. Obsahově ale postrádá detailnější rozbor současného stavu - rešerši a taktéž praktické řešení je v rovině spíš bakalářské práce.

Otázky k obhajobě

Na základě čeho jste volili detekční pravidla k implementaci?
Jak probíhalo testovaní pravidel?

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.

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.