FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Simona Fornůsek, Ph.D.
Student:	Bc. Stanislav Lepič
Název práce:	Detekční Pravidla pro Detekci Ransomware ve Formátech YARA a Sigma
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

Byť jsou všechny body zadání formálně naplněny, přístup k práci je poměrně povrchní.
V teoretické části mi chybí detailnější rešerše jednotlivých rodin ransomware a identifikace jejich znaků chování, a to jak unikátních, tak i obecných, využívaných napříč různými rodinami ransomware. Kapitola 1.2 se sice věnuje chování ransomware, ale jedná se spíše o obecný popis, než systematickou rešerši.

Rovněž přístup k praktické části je poměrně naivní. Pro logování událostí ze systému student zvolil nástroj sysmon a logy OS Windows (což by bylo zcela v pořádku), u kterých ale zapíná logování poměrně velkého množství událostí v systému, které ani nevypadají použity pro další detekci - což není úplně efektivní, a u produkčně používaného systému by bylo nutné otestovat limity zdrojů systému. Detekce vytvořené v rámci práce jsou v pořádku, nicméně chybí systematičtější přístup, nejspíš i kvůli chybějící teoretické rešerši. Zároveň jsou veškeré detekce zaměřeny na již pokročilou fázi běhu ransomware, zcela chybí detekce úvodních fázi jako např. exploitace, instalace. Testování a vyhodnocení by také zasloužilo více pozornosti.

2. Písemná část práce

59 / 100 (E)

Jak již bylo zmíněno v předchozím bodě, práce klouže po povrchu problematiky. Diplomová práce by zasloužila systematičtější přístup, detailnější rešerši a rozbor jednotlivých rodin ransomware, identifikaci chování k detekci, i systematičtější přístup k tvorbě detekcí. Velká část diplomové práce popisuje pouze obecné poznatky ohledně

malware - ať již kapitola 1.2., či rovněž kapitola 2 sice nadepsána jako "Analýza ransomware", nicméně popisuje pouze obecné možnosti analýzy malware.

3. Nepísemná část, přílohy 65 /100 (D)

Přiložené jsou soubory s detekčními pravidly, to je v pořádku. Chybí nicméně detailnější popis konfigurace testovacího prostředí, který by umožnil snadnou opakovatelnost, rovněž chybí detaily k výsledkům testování.

4. Hodnocení výsledků, jejich využitelnost 59 /100 (E)

Implementované detekce jsou v pořádku a mohly by být použity v praxi, nicméně, pro obecnější detekci ransomware by bolo potřeba systematičtějšího přístupu a pokrytí širší škály detekcí.

5. Aktivita studenta

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

6. Samostatnost studenta

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

Celkové hodnocení 59 /100 (E)

V rámci diplomové práce bych očekávala detailnější a systematičtější přístup k zpracování rešerše a následně i k praktické implementaci detekčních pravidel. Předložená práce spíše klouže po povrchu problematiky, a obsahuje mnoho obecných částí.
Nicméně, všechny body zadání byly do jisté míry splněny, a proto bych práci doporučila 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.