FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	prof. Ing. Róbert Lórencz, CSc.
Student:	Bc. Martin Mandík
Název práce:	Techniky perzistence malware a její detekce
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

Zadání bylo splněné bez výhrad.

2. Písemná část práce 90 / 100 (A)

Písemná část práce je obšírná, čtenáře poměrně detailně seznamuje s problematikou perzistence malware, i aktuálně používanými technikami.
Trochu nejasné je, jak student zvolil techniky k implementaci (ne všechny techniky popsané v kapitole 2.1 byly nakonec implementovány). Zároveň není úplně jasně představen popis GRR workflows sběru dalších artefaktů ani jejich přesný obsah.
Vyhodnocení by mohlo být ještě doplněno o zhodnocení pokrytí technik ve srovnání s MITRE ATT&CK frameworkem.

3. Nepísemná část, přílohy 96 / 100 (A)

V přílohách student přikládá konfiguraci prostředí, což umožňuje opakovatelnost experimentů, i další praktické použití.

4. Hodnocení výsledků, jejich využitelnost 93 / 100 (A)

Vytvořené pravidla jsou prakticky využitelné. Rovněž návrh řešení integrující detekční mechanismus a sběr artefaktů pro další analýzu najde praktické uplatnění.

Celkové hodnocení

95 /100 (A)

Zvolené téma je vysoce aktuální a dobře zpracované. Práce je obsahově bohatá, zvoleným technikám se student věnuje detailně. Navrhované řešení je smysluplné prakticky využitelné a vybrané nástroje pro implementaci jsou aktuální.

Otázky k obhajobě

Jak přesně jste volil techniky k implementaci detekcí?
Jaký rozsah artefaktů je pokrytý v rámci GRR workflows, a jak by mohly být dále využity?

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.