FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Jan Suchara
Vedoucí: práce: Ing. Tomáš Čejka, Ph.D.
Název práce: Evaluation of captured flow data of suspicious devices
Obor: Bezpečnost a informační technologie

Datum vytvoření: 10. 6. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
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.

Komentář:
Všechny plánované cíle se podařilo naplnit. V rámci práce vzniklo několik výstupů nad rámec zadání bakalářské práce. Tyto výstupy jsou využitelné v ostatních modulech open source systému NEMEA pro analýzu síťového provozu a detekci anomálií.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*85 (B)*

Popis kritéria:
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. 26/2017, 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.

Komentář:
Práce je vypracována v anglickém jazyce, jazykově je na vysoké úrovni. Text je srozumitelný, obsahuje všechny podstatné části, je informačně bohatý. Práce obsahuje typografické nedostatky a na několika místech nejsou správně řešené odkazy.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*89 (B)*

Popis kritéria:
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

Komentář:
Vytvořené nástroje byly otestované a jsou funkční. Zdrojové kódy by bylo vhodné vylepšit a to doplněním komentářů a zadefinováním nalezených konstant, které tvoří základ rozhodovacího algoritmu. Je škoda, že na přiložené CD student nepřidal i skript v jazyce R, kterým byly nalezeny hodnoty prahových hodnot.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*99 (A)*

Popis kritéria:
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.

Komentář:
Vytvořené nástroje split_evidence a evaluator jsou použitelné v praxi pro vyfiltrování bezpečnostních událostí, které se statisticky podobají provozu generovanému malwarem. Navíc se během vypracování bakalářské práce podařilo připravit konferenční příspěvek.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 5b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
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 (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student na závěrečné práci pracoval velice intenzivně a díky vyvinutému úsilí se podařilo vytvořit velice kvalitní bakalářskou práci. Student se účastnil pravidelných schůzí výzkumného týmu, na které byl vždy dobře připraven.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*95 (A)*

Popis kritéria:
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.

Text hodnocení:

Přes drobné nedostatky má odevzdaná práce vysokou kvalitu. Text práce je vypracován v anglickém jazyce a obsahuje pouze drobné nedostatky. Výsledkem jsou funkční nástroje přičemž hlavním přínosem je modul Evaluator, který slouží k vyfiltrování IP adres, které komunikují se serverem na blacklistu a jejich chování se statisticky podobá zařízením nakaženým malwarem. Obsah práce se podařilo popsat v příspěvku na prestižní mezinárodní konferenci IMC, o jehož přijetí/nepřijetí zatím nemáme informace.

Podpis vedoucího práce: