FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Maxmilián Tomáš
Oponent práce:	Ing. Pavel Benáček, Ph.D.
Název práce:	Rozšíření reputační databáze o informace z Passive DNS
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 5. 6. 2018

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* *2=náročnější zadání,* ***3=průměrně náročné zadání,*** *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Student nastudoval technologii DNS, seznámil se s přístupem Passive DNS a systémem pro evidenci reputace síťových entit Network Entity Reputation Database (NERD). Následně provedl návrh a rozšíření systému NERD o podporu Passive DNS, provedl testování a nasazení systému nad reálným provozem. Student se z větší části inspiroval z existujícího článku, který následně implementoval. Z tohoto důvodu hodnotím zadání jako průměrně obtížné.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. 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 splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Všechny body zadání byly splněny.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	*1=splňuje požadavky,* ***2=splňuje požadavky s menšími výhradami,*** *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Jednotlivé části textu jsou informačne dostatečné až na část testování. Tato část by mohla obsahovat podrobnější testování výkonosti a rychlosti importu dat.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*85 (B)*

Popis kritéria:
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.

Komentář:
Některé kapitoly obsahují drobné nepřesnosti (například že nástroj vagrant je virtuální stroj). Z tohoto důvodu hodnotím věcnou a logickou úroveň známkou B, protože i s těmito nepřesnostmi je text stále kvalitní.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*60 (D)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Komentář:
Po jazykové stránce obsahuje text velký počet překlepů, které zhoršují čitelnost textu. Po typografické stránce obsahuje práce nesjednocené formátování tabulek, popisu obrázků, použitých knihoven a podobně. Kvůli velkého počtu překlepů a nesjednocenému formátování je čtení textu obtížnější. Z uvedených důvodů hodnotím formální úroveň práce známkou D.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*75 (C)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Všechny použité části jsou citovány a řádně odlišeny od vlastních výsledků. V některých částech textu by bylo vhodné uvést citaci na použité knihovny a použité blacklisty tak, aby bylo možné jednodušeji dohledat více informací. Navíc citace neodpovídají české citační normě.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*100 (A)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Vytvořený modul je funkční a nasazen do systému pro evidenci reputace síťových entit Network Entity Reputation. Student tedy splnil veškeré body zadání. Z uvedených důvodů hodnotím známkou A.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Výsledkem práce je modul do systému NERD, který je využíván odborníky v oblasti bezpečnosti. Procento využití v praxi je tedy poměrně vysoké.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
Na studenta mám následující otázku:

Výsledkem práce je modul pro podporu Passive DNS v systému pro evidenci reputace síťových entit Network Entity Reputation Database (NERD). Plánujete nasadit tento druh detekce i do jiných sytémů jako je například NEMEA (viz. odkaz https://github.com/CESNET/Nemea)?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*79 (C)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Student nastudoval a implementoval modul pro Passive DNS do systémemu pro evidenci reputace síťových entit Network Entity Reputation Database (NERD). Zadání samotné práce bylo splněno ve všech bodech. Ve svém hodnocení jsem musel přihlédnout k formální a typografické úrovni práce, která obsahuje velké množství překlepů a nesjednocené formátování. Výsledkem je však funkční modul do systému NERD a proto jsem se rozhodl práci hodnotit známkou C - dobře.

Podpis oponenta práce: