FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Lenka Stejskalová
Oponent práce:	Ing. Václav Bartoš
Název práce:	Systém pro evidenci podezřelých skupin síťových adres
Obor:	Počítačová bezpečnost

Datum vytvoření: 4. 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:
Zadáním je vytvořit systém zpracovávající hlášení o škodlivém chování IP adres a slučování těchto adres do skupin podle podobnosti jejich chování. Zadání je obtížné, protože příchozí hlášení jsou velmi různorodá, je jich velké množství a vyhledávání podobností v datech je obecně náročný úkol.

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:
Výsledkem je funkční platforma pro ukládání informací o skupinách adres. Implementované metody vyhledávání skupin však nejsou navrženy příliš dobře (jádrem zadání však byla především platforma pro ukládání, proto je to jen drobná výhrada).

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:
Kapitoly Návrh řešení a Implementace se z velké části překrývají a uvádí znovu stejné informace. Naopak některé důležité informace v práci chybí (např. podrobnosti o tom, podle čeho se IP adresy shlukují do skupin, či vyhodnocení propustnosti v kap. Testování). Celkově je práce spíše kratší, stále však v rámci doporučeného rozsahu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*50 (E)*

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:
Zejména v první části (úvod do problematiky) je řada nepřesností či zavádějících informací. V některých ohledech je práce nelogicky organizovaná (např. vysvětlení algoritmu seskupování adres je až na samém konci kapitoly Implementace, pochopení zbytku práce by výrazně pomohlo, kdyby byl algoritmus uveden hned na začátku). Některé části textu jsou hůře pochopitelné. Jiné části jsou však v pořádku a vše podstatné se z textu vyčíst dá. Celkově je kvalita textu nízká, ale dostatečná.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*75 (C)*

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 typografické a formální stránce je práce v pořádku. Jazykově je práce spíše podprůměrná.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*85 (B)*

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:
Literatura odkazovaná v úvodu do problematiky se téměř výhradně skládá z internetových článků a příspěvků na blozích. Vzhledem k tématu to však příliš nevadí a vybrané zdroje jsou poměrně kvalitní. Bibliografické citace jsou v pořádku a převzaté pasáže jsou vždy řádně označeny.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*65 (D)*

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:
Navržená architektura systému je robustní a připravená na vysokou zátěž. Navržený datový model však není ideální a především konkrétní metody slučování IP adres do skupin jsou zatím jen velmi jednoduché a před použitím v praxi je ještě bude nutné značně vylepšit.

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:
Výsledek práce zatím není přímo použitelný v praxi. To je však z velké části dáno i nedostatečnou kvalitou vstupních dat (což není chyba studentky). Vytvořený SW je nicméně užitečná platforma, z níž může v blízké budoucnosti vzniknout velmi přínosný systém.

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:
* Je možné do systému zapojit i jiné zdroje dat, než IDEA zprávy ze systému Warden?
* Plánujete na vývoji systému dále pracovat? Pokud ano, co plánujete jako hlavní vylepšení?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*65 (D)*

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:
Textová část práce má řadu nedostatků. Implementovaný software je v mnoha ohledech kvalitní, některé části jsou však "nedotažené". To je ale částečně dáno nízkou kvalitou dat, které měla studentka k dispozici, navíc zadání bylo poměrně obtížné. Celkově lze přes všechny nedostatky zadání hodnotit jako splněné.

Podpis oponenta práce: