FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Bc. Lenka Stejskalová
Vedoucí práce: Ing. Tomáš Čejka
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:
Práce se zabývá obtížným tématem automatického vyhodnocování informací o bezpečnostních událostech a dalších informací o síťových entitách. Cílem práce bylo na základě analýzy dostupných dat navrhnout a vytvořit prototyp systému, do kterého je možné ukládat skupiny entit, které se chovají podezřele a vykazují podobné chování.

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 práce je funkční prototyp systému pro evidování podezřelých skupin entit. Vzniklý systém přijímá data z externích zdrojů, zpracovává je a v pravidelných intervalech odmazává stará data.

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:
Práce obsahuje informačně bohaté části, neobsahuje zbytečné části.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*69 (D)*

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:
Práce má logickou strukturu, kapitoly na sebe navazují, text je pro čtenáře víceméně pochopitelný. Implementační část textu práce by mohla obsahovat více technických detailů. Přiložené zdrojové kódy na CD nejsou dostatečně okomentovány; domnívám se, že některé kusy kódu nejsou řešeny efektivně vzhledem k použitým technologiím; zdrojové kódy zřejmě obsahují autentizační token, který by měl být uložen v konfiguračním souboru mimo verzované zdrojové soubory.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*85 (B)*

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:
Práce obsahuje drobné typografické chyby, které nenarušují čitelnost práce. Použití uvozovek uvnitř uvozovek na str.9 je nezvyklé.

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:
Práce by mohla citovat více relevantních publikovaných článků. Autor u citace [14] by měla být spíše organizace CESNET. Uvedené citované zdroje jsou správně použity v textu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*90 (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:
Výstupem práce je funkční prototyp systému pro evidenci podezřelých skupin síťových entit. Tento systém bude základem pro budoucí výzkum a vývoj a je plánováno ho využit jako zdroj důležitých informací pro vyhodnocování bezpečnostních incidentů a pro automatickou mitigaci síťových útoků. Tato práce má do budoucna publikační potenciál.

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 této práce (systém pro evidenci skupin podezřelých entit) je využitelný v praxi. Díky vytvořenému API je možné použít uložené informace v ostatních systémech a nástrojích.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 9b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:
Studentka pracovala samostatně, byla schopná řešit objevené problémy spojené s řešením této práce a flexibilně upravovat a vylepšovat návrh systému v průběhu řešení. Studentka se účastnila pravidelných schůzí týmu, na které byla vždy dobře připravena.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*70 (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:
Zadání práce bylo splněno a výsledkem je funkční prototyp systému pro evidenci užitečných informací o skupinách síťových entit. Jedná se tak o doplněk existujícího systému (NERD), který se aktuálně zabývá evidováním historického chování samostatných síťových entit bez ohledu na jakoukoliv podobnost mezi entitami. Tato diplomová práce je důležitým stavebním kamenem pro budoucí výzkum v oblasti automatické analýzy a vyhodnocení bezpečnostních událostí.

Podpis vedoucího práce: