Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Bc. Petr Lessner
Vedoucí práce: Mgr. Rudolf Bohumil Blažek, Ph.D.
Název práce: Detekce anomálií síťového provozu pomocí data miningové analýzy síťových toků
Obor: Počítačová bezpečnost

Datum vytvoření: 1. 2. 2016

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:
Zadání považuji za náročnější, protože zahrnuje nejen analýzu, výběr a implementaci metody pro detekci behaviorálních anomálií v síťovém provozu, ale i experimentální výběr a následný návrh použitých agregovaných charakteristik síťového provozu. Výběr agregovaných charakteristik provozu patří mezi nejobtížnější kroky behaviorální analýzy v síťové bezpečnosti.

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:
Student splnil všechny body zadání práce. Nad rámec zadání student detekoval skutečné anomálie a pravděpodobné pokusy o útok v provozu z reálné počítačové sítě.

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:
Předložená ZP svým rozsahem splňuje požadavky a neobsahuje žádné zbytečné části. Všechny její části jsou dostatečně podrobné.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*92 (A)*

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 je po logické a věcné stránce vypracována velmi kvalitně.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*89 (B)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 12/2014, článek 3.

Komentář:
Práce má velmi dobrou formální a jazykovou úroveň, snad jen popis některých metod by zasloužil více podrobností místo odkazů na detaily v literatuře, především pro úsporu času čtenáře.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*90 (A)*

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 obsahuje velmi četné odkazy na 80 zdrojů, z čehož 14 jsou publikace z vědeckých konferencí a časopisů. Zbylé zdroje se týkají použitých technologií a proto jsou často online, jakožto součást veřejně dostupné dokumentace či standardů. U vědecké práce tohoto rozsahu by některé technické odkazy mohly být vynechány a některé vědecké mohly být doplněny. Avšak pro diplomovou práci, jejíž součástí je implementace zásuvného modulu pro existující detekční systém, práci se zdroji považuji za adekvátní a hodnotím ji jako výbornou.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*95 (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:

Student vybral kvalitní a pokročilé data miningové metody pro porovnávání podobnosti chování hostů sledované počítačové sítě i pro detekci neobvyklého chování. Zároveň vybral agregované charakterostiky provozu, které během testování vedly k detekci několika skutečných anomálií a pravděpodobných pokusů o útok. Implemetovaný zásuvný modul je funkční a prakticky použitelný. Výsledky práce proto považuji za netriviální.

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:

Implementovaný zásuvný modul je funkční a lze ho nasadit v provozu běžně používané opensourcové softwarové síťové sondy NfSen. Použité detekční metody a charakteristiky provozu jsou prakticky využitelné pro detekci behaviorálních anomálií na základě monitorování síťových toků NetFlow a IPFIX. Zásuvný modul je součástí širšího projektu výzkumné skupiny síťové bezpečnosti na FIT ČVUT v Praze, jehož cílem je umožnit statistickou detekci anomálií v běžně používaných detekčních systémech. Budoucím studentům umožní nasazení a testování nových statistických metod pro detekci anomálilí v realistickém síťovém prostředí. Představuje tak důležitý prvek pro rozvoj výzkumu v oblasti síťové bezpečnosti na naší fakultě.

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:

Student byl výjimečně aktivní a velmi samostatný. Na schůzky docházel pravidelně a vždy dobře připraven.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*96 (A)*

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:

Výsledky práce považuji za výjimečně užitečné nejen pro aplikovaný výzkum síťové bezpečnosti na naši fakultě, ale poteniálně i pro projekt síťové sondy NfSen. Prezentovaná funkčnost modulu je příslibem jeho budoucího využití.

Podpis vedoucího práce: