

Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze

Fakulta informačních technologií

Student: Bc. Marek Krátký
Vedoucí práce: Mgr. Rudolf Bohumil Blažek, Ph.D.
Název práce: Turris plugin pro analýzu síťového provozu pomocí statistických metod
Obor: Počítačová bezpečnost (magisterský)

Datum vytvoření: 4. 6. 2015

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: Cílem práce byl návrh a implementace zásuvného modulu pro routery a síťové sondy Turris sdružení CZ.NIC, který umožní nasazení pokročilých statistických detekčních metod v těchto sondách. Zvláštní důraz byl kladen na otestování vybrané statistické metody ve virtualizovaném prostředí sondy Turris a ověření tak využitelnosti zásuvného modulu pro reálné nasazení v distribuovaném prostředí těchto sond. Důležitým aspektem práce byla snadná rozšiřitelnost modulu o nové statistické metody v budoucnosti.	
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 dosáhl schválení vytvořeného modulu pro testování a následné reálné nasazení na sondách v rámci projektu Turris sdružení CZ.NIC.	
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 všechny její části jsou dostatečně podrobné. Práce neobsahuje žádné zbytečné části.	
Hodnotící kritérium:	Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):
4. Věcná a logická úroveň práce	90 (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 věcné stránce napsána odpovídajícím způsobem, má dobrou logickou strukturu a neobsahuje žádné závažné věcné chyby ani nepřesnosti, i když místy by si zasloužila preciznější formulace.	
Hodnotící kritérium:	Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):
5. Formální úroveň práce	90 (A)
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:

Z formálního hlediska je práce napsána kvalitně, bez závažných jazykových prohřešků. Má však některé nepříliš podstatné typografické nedostatky, např. fragmenty slov či vět na konci odstavce. Viz str. 7, odst. 2, nebo méně závažné prohřešky str. 3, odst. 1 nebo str. 4, odst. 1. Obrázek 1.6 na str. 25 by bylo vhodnější zmenšit a umístit na předchozí stranu spolu s textem.

Hodnotící kritérium:

Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):

6. Práce se zdroji

95 (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 se zdroji je na velmi vysoké úrovni a odpovídá vědecké publikaci.

Hodnotící kritérium:

Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):

7. Hodnocení výsledků, publikační výstupy a ocenění

93 (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:

Implementace zásuvného modulu pro sondy Turrís sdružení CZ.NIC byla provedena v souladu se specifikacemi projektu Turrís, takže modul byl předběžně schválen pro testování v rámci projektu sdružení CZ.NIC na sondách Turrís, které jsou instalovány v testovací laboratoři, a následně i na sondách v sítích koncových uživatelů routerů Turrís. Výsledkem je zásuvný modul, který byl otestován s daty z reálného provozu. Tento modul je použitelný v rámci projektu Turrís sdružení CZ.NIC pro testování statistických detekčních metod.

Hodnotící kritérium:

Způsob hodnocení - nehodnotí se

8. Komentář o využitelnosti výsledků**Popis kritéria:**

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

Komentář:

Výsledný 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 systémech pro detekci síťových útoků a anomálií. Budoucím studentům umožní testování nových distribuovaných statistických metod pro detekci anomálií ve spolupráci se sdružením CZ.NIC. Tato ZP tak představuje 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 samostatně tvůrčí práce (9b).

Komentář:

Student byl výjimečně aktivní a 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

93 (A)

Popis kritéria:

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

Text hodnocení:

Výsledky práce považuji za užitečné pro aplikovaný výzkum síťové bezpečnosti na naší fakultě, se zaměřením na distribuované systémy pro detekci síťových anomálií. Předběžné schválení vytvořeného zásuvného modulu pro testování v rámci projektu Turrís sdružení CZ.NIC je příslibem budoucího využití modulu a přispívá k rozvoji spolupráce naší fakulty s bezpečnostní komunitou IT v ČR.

Podpis vedoucího práce: