Posudek oponenta závěrečné práce

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

Student: Otto Hollmann
Oponent práce: Ing. Václav Bartoš
Název práce: Detekce síťových útoků typu Denial of Service
Obor: Teoretická informatika

Datum vytvoření: 3. 6. 2017

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 je průměrně obtížné.
Je součástí většího projektu - konkrétně jde o modul do existujícího systému pro analýzu síťových dat. Jeho výsledky by měly být použity v praxi na reálné síti pro detekci DDoS útoků.

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:
Úvod a analýza útoků a stávajících řešení má vhodný rozsah. Některé části popisu detekčního algoritmu by však měly být podrobnější. V práci je sice množství diagramů popisujících fungování modulu, často však bez dostatečného doprovodného textu. Chybí popis některých detailů algoritmu či možností konfigurace a celkově je fungování modulu nedostatečně vysvětleno.

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:
V teoretickém úvodu práce je několik drobných faktických nepřesností, které však nejsou příliš významné.
Největší slabinou práce je její logická struktura a (ne)srozumitelnost pro čtenáře, zejména v části popisu algoritmu a implementace. Mnoho aspektů fungování modulu či parametrů algoritmu není vysvětleno, případně je vysvětleno v textu později, než je na ně odkazováno.

Typickým příkladem je např. sekce 3.2.1 pojednávající o tom, co se stane "při každé aktualizaci záznamu". To, o jaké záznamy jde a jakým způsobem se aktualizují se však čtenář dozví až v kapitole 4.1 (popis implementace).

Dále např. důležitý fakt, jak se záznamy z datových struktur odstraňují, je zmíněn jen velmi stručně u popisu parametrů programu.

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. 14/2015, článek 3.

Komentář:
Práce obsahuje několik překlepů a jiných drobných chyb, jinak je po formální stránce v pořádku.

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:
Studijní zdroje jsou vzhledem k charakteru práce zvoleny dobře. Všechny převzaté části jsou správně citovány a odlišeny od vlastní práce. Formátování citací je v pořádku. Jen odkazy na webové stránky různých projektů a softwaru mohly být řešeny spíše pomocí poznámek pod čarou než bibliografickými citacemi.

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:
Vyvinutý modul je implementován kvalitně, je plně funkční a zcela splňuje zadání. V současnosti je nasazen pro analýzu dat ze sítě CESNET2 a poskytuje dobré výsledky.

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:
Vyvinutý modul se v současnosti testuje na síti CESNET2 a pravděpodobně bude využíván v praxi pro detekci DDoS útoků.

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:
- Popište, jak probíhá hlášení déle trvajícího útoku (na začátku, na konci, průběžně opakovaně?).
- Jak rychle dokáže modul útok detekovat? Na čem délka detekčního zpoždění závisí?

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:
Implementovaný modul pro detekci DDoS útoků je velmi kvalitní a funguje dle očekávání. Plánuje se jeho použití v praxi pro detekci útoků v síti CESNET2. Slabinou práce je textová část, zejména popis algoritmu, který je nedostatečně podrobný a špatně organizovaný. Celkově navrhuji hodnocení stupněm C.

Podpis oponenta práce: