Posudek oponenta závěrečné práce

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

Student: Libor Šlechta
Oponent práce: Ing. Jiří Smítka
Název práce: Detekce pomalých útoků hrubou silou
Obor: Informační technologie

Datum vytvoření: 17. 6. 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:
Průměrně náročné zadání

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:
Zadání splněno

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 splňuje požadavky.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*89 (B)*

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 dobře strukturovaná a neobsahuje věcné chyby. Text je dobře pochopitelný, zdrojové texty jsou přehledné a komentované. Autor se v celé práci nezmínil o jiných metodách prevence před útoky hrubou silou, v případě SSH např. přihlašování pomocí klíčů (hlavně v kap. 2.1).
Testy, které autor provedl, jsem nemohl zopakovat, neboť testovací datové sady nejsou přiloženy na CD. To lze však, vzhledem k jejich citlivé povaze, pochopit.

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. 12/2014, článek 3.

Komentář:
Práce splňuje typografické i jazykové požadavky. V práci jsem nenalezl naprosto žádné překlepy. Autor občas trochu plýtvá podkapitolami, v práci je např. podkapitola 7.1.2.1 aniž by existovala 7.2.1.2. Tento jev je na více místech. Podkapitoly třetí a čtvrté úrovně nejsou uvedeny v obsahu.

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:
Autor nepokryl zdroji problematiku pomalých distribuovaných slovníkových útoků s obhajobou, že nenalezl žádné řešení (viz 3.1). Výsledky v tomto smyslu může přinést např. analýza záznamů o síťových tocích, viz např.:
VYKOPAL, Jan, Tomáš PLESNÍK a Pavel MINAŘÍK. Network-based Dictionary Attack Detection. In Proceedings of International Conference on Future Networks (ICFN 2009). Los Alamitos, CA, USA: IEEE Computer Society, 2009. s. 23-27, 5 s. ISBN 978-0-7695-3567-8.
Jinak je práce zdroji pokryta, autor se na jednotlivé prameny v textu odkazuje.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*85 (B)*

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:
Autor implementoval aplikaci dle požadavků v zadání práce. Aplikace je funkční a lze ji relativně snadno nainstalovat a používat.

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:
Podle tvrzení autora se jedná o jedinou implementaci detektoru tohoto druhu. Toto nejsem schopen z časových důvodů potvrdit, bylo by třeba kontaktovat více autorů různých článků na toto téma. Nicméně v každém případě vznikla aplikace, která je bezesporu přínosem pro administrátory serverů v Internetu.

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:
Dohledal jste před obhajobou nějakou existující aplikaci srovnatelnou s Vaší prací ? Můžete tato řešení porovnat ? Prosím minimálně o srovnání s řešením problému pomocí rozhodovacího stromu ve zdroji uvedeném v posudku bodě 6 (autor je mimochodem stejný jako u zdroje [6]).

Můžete, prosím, popsat použité datové sady využité pro testování ? V práci chybí např. rámcová informace o počtech přistupujících legálních uživatelů a počtech jimi využitých IP adres. Zajímavá by byla i informace o průměrném počtu záznamů za den.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*85 (B)*

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:
Autor splnil zadání bakalářské práce. Práce je pro administrátory sítí přínosná.

Podpis oponenta práce: