Hodnocení vedoucího závěrečné práce

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

Student: Libor Šlechta
Vedoucí práce: Mgr. Jan Starý, Ph.D.
Název práce: Detekce pomalých útoků hrubou silou
Obor: Informační technologie

Datum vytvoření: 18. 5. 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:
Detekce distribuovaných útoků je dosud předmětem výzkumu. Kromě samotné implementace se autor musel seznámit s netriviální literaturou a celým použitým matematickým aparátem.

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:
Formálně není splněn bod 2, totiž implementace v předepsaném jazyce C.
Autor implementoval detektor útoků v jazyce Python, se souhlasem školitele.
Jakmile došla volba konkrétního řešení ke článku [1], který využívá statistickou nalýzu logů, padla většina důvodů pro použití jazyka C (který by naopak byl samozřejmým nástrojem při zachytávání paketů živého provozu). Řešení není touto volbou nijak umenšeno.

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:
Rozsah práce je odpovídající a všechny její části jsou relevantní.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*85 (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 sepsána pečlivě. Statistický úvod, tj. popis CUSUM algoritmu (kumulativní suma odchylky od střední hodnoty), by však bylo možné podat podrobněji.

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:
Typograficky, formálně a jazykově je práce 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:
Práce cituje dvanáct zdrojů, především původní články [12] a [1], jejichž algoritmy implementuje.
Ostatní jsou relevantní odkazy na práce o síťových útocích a použitý statistický aparát.
Slajdy z BI-PST by zřejmě bylo možné nahradit nějakou standardní učebnicí statistiky.

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:
Hlavním výsledkem je prototyp detektoru distribuovaných SSH útoků, vycházející z algoritmů
popsaných v původním článku "Detecting stealthy, distributed SSH brute-forcing" [1].
Místo popsaného beta-binomiálního rozdělení pravděpodobnosti používá práce jako zjednodušení jen binomiální rozdělení.
Zobecnit detector pro jiná zobecnění znamená nahradit funkci binomial() Pythonovské knihovny NumPy jinou funkcí,
a výsledek práce tím není nijak umenšen.

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 detektor lze chápat jako příspěvek k dosud probíhajícímu výzkumu.
Jeho praktickou použitelnost lze zvážit teprve po nasazení na netriviální ostrá data,
tj. logy SSH serverů s netriviálním provozem a počtem uživatelů - které však typicky
nejsou k dispozici. Autoři původního článku provedli svou statistickou analýzu na 8 letech
kompletních SSH logů celého Berkeley campusu (přibližně 2000 SSH serverů), které nám neposkytli.
Na skromnějších datech, která měl autor k dispozici (jaro 2016 na fray.fit.cvut.cz, rok 2015 na stary.fit.cvut.cz),
dává detektor rozumné výsledky. V textu práce jsou uvedeny konkrétní ukázky detekovaných útoků.

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:
Řešitel pracoval zcela samostatně, na pravidelné konsultace byl vždy připraven.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*90 (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:
Vzhledem k náročnosti zadání navrhuji stupeň A.

Podpis vedoucího práce: