FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Bc. Filip Šuster
Vedoucí: práce: Ing. Tomáš Čejka, Ph.D.
Název práce: Automatická detekce podezřelého síťového provozu pomocí blacklistů
Obor: Počítačové systémy a sítě

Datum vytvoření: 27. 1. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. 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 dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Komentář:
Cílem závěrečné práce je analýza flow dat v reálném čase založená na veřejně dostupných seznamech podezřelých/škodlivých adres. Výsledkem práce je skupina funkčních nově vytvořených nebo vylepšených NEMEA modulů, které slouží k automatickému spouštění záchytu dat a dodatečné analýze.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*75 (C)*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále 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. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Komentář:
Text závěrečné práce je dobře členěný, obsahuje důkladnou analýzu problematiky a pečlivě vysvětluje motivaci pro adaptivního filtrování, které má za cíl zachytit flow data podezřelých klientů pro předzpracování a vyhodnocení potenciálních falešně pozitivních alertů. Text obsahuje drobné nepřesnosti, které nenarušují celkové porozumění. Text obsahuje typografické chyby.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*88 (B)*

Popis kritéria:
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce
– opakovatelnost experimentů

Komentář:
Hlavním výstupem této závěrečné práce je poměrně komplexní sada nově vytvořených nebo významně vylepšených nástrojů - NEMEA modulů, které vykonávají 1) filtrování flow dat v reálném čase podle IP/DNS/URL blacklistů, 2) agregování vyfiltrovaných dat podle řady kritérií s cílem vytvořit menší počet hlášení obsahujících související provoz 3) adaptivní filtrování, tzn. modul, kterému se dynamicky mění seznam sledovaných adres, 4) vytváření hlášení bezpečnostních hlášení pro odeslání do systému Warden.
Zdrojový kód je napsaný přehledně, ale bylo by vhodné doplnit dokumentaci.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*100 (A)*

Popis kritéria:
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Komentář:

Výsledkem práce je použitelná sada softwarových nástrojů, která je nyní součástí open source systému NEMEA. Aktuálně jsou vytvořené moduly spuštěné na produkčním serveru sdružení CESNET, na kterém se analyzují flow data z perimetru národní akademické sítě CESNET2. Výsledky jsou tudíž využitelné v praxi. Myšlenka adaptivního filtrování na úrovni flow dat včetně návrhu byly prezentovány v rámci příspěvku na mezinárodní konferenci PESW 2018.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 5b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student pracoval aktivně a samostatně. Během spolupráce se student plně zapojil do činností výzkumného týmu, a byl cenným přínosem nejen výsledky své práce, ale poskytoval navíc konzultace a zpětnou vazbu dalším členům týmu.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*90 (A)*

Popis kritéria:
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

Text hodnocení:

Předložená práce je celkově na dobré úrovni, myšlenka adaptivního filtrování a zpracování zachycených dat byla prezentována a diskutována v rámci odborné komunity na konferenci PESW 2018. Text práce i vytvořené zdrojové kódy jsou logicky členěny a přehledně zpracovány, ale přesto by bylo vhodné zapracovat na drobných nedostatcích jako je např. vylepšení dokumentace.

Podpis vedoucího práce: