FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Jan Neužil
Vedoucí: práce:	Ing. Tomáš Čejka, Ph.D.
Název práce:	Network devices and services Identification using passive monitoring
Obor:	Počítačová bezpečnost

Datum vytvoření: 24. 8. 2020

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:

Práce se zabývá problematikou pasivního monitorování a interpretace síťového provozu. Cílem je identifikovat sadu scénářů, pro které je možné síťovým operátorům poskytnout srozumitelnější informace o smyslu/účelu síťového spojení. Výsledkem práce je důkladná analýza protokolů pro automatické objevování zařízení a jejich služeb a funkční prototyp analyzátoru síťové komunikace, který přiřazuje spojením štítky reprezentující význam spojení. Vyvinuté nástroje byly otestovány nad vytvořenými ukázkovými datovými sadami.

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

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 práce je v angličtině na vynikající úrovni. Práce neobsahuje žádné zásadní jazykové nebo typografické problémy. Práce obsahuje dostatečné množství relevantních citovaných zdrojů.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*85 (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:

Výsledkem práce je sada skriptů, které umožňují zpracovat pasivně monitorovaný provoz lokálních počítačových sítí. Vyvinutý prototyp byl otestovaný na provozu z reálné sítě a navržené scénáře ukazující užitečnou přidanou informaci pro síťové operátory/uživatele. Dokumentaci zdrojových kódů by bylo vhodné ještě vylepšit.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*95 (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:

Práce se zabývá analýzou a párováním informací z různých zdrojů, tzn. z různých komunikačních protokolů, které prozrazují podrobnosti o aktivních zařízeních na lokálních sítích. Na základě navrženého mechanismu vyhodnocování dat byl vytvořen prototyp analytického modulu, který automaticky odhaduje důvod komunikace. Tento přístup představuje přínos pro analytika síťového provozu oproti stávajícím nízko-úrovňovým informacím o protokolech a paketech. Výsledky jsou využitelné v praxi.

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 odvedl značný kus práce na vytváření testovacího prostředí pro záchyt datových sad a experimenty s analýzou provozu. V průběhu řešení této diplomové práce se intenzivně zapojil to výzkumu/vývoje v rámci Laboratoře monitorování síťového provozu.

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:

Odevzdaná diplomová práce je v anglickém jazyce a její zpracování je velice kvalitní. Výsledkem je zajímavý přístup k pasivnímu monitorování a interpretace pozorovaného síťového provozu. Na základě vytvořeného prototypu je zřejmé, že výsledné informace, jež jsou výstupem vyvinutých softwarových modulů, jsou užitečné v praxi pro síťové operátory a bezpečnostní analytiky, jejichž cílem je interpretovat provoz na síti.

Podpis vedoucího práce: