FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jan Luxemburk
Student:	Tomáš Klatovský
Název práce:	Detekce síťového provozu aplikace TeamViewer
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	26. května 2021

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

Zadání hodnotím jako průměrně těžké a bylo zcela splněno.

2. Písemná část práce 90/100 (A)

Práce se věnuje aktuálnímu tématu zkoumání šifrovaného síťového provozu, a to pro aplikaci TeamViewer.

Struktura práce je dobrá a rozsah jednotlivých částí je přiměřený. Po věcné stránce je práce až na několik drobností v pořádku. Práce je psaná v angličtině a jazykovou kvalitu hodnotím jako velmi dobrou.

Seznamu použité literatury lze vytknout, že obsahuje pouze 2 odborné články. Zbytek tvoří příspěvky na blozích, RFC dokumenty, závěrečné práce jiných studentů, a hlavně odkazy na použité knihovny a software. Tyto zdroje lze však vzhledem k charakteru práce očekávat.

3. Nepísemná část, přílohy 80/100 (B)

V rámci nepísemné části práce obsahuje skript na předzpracování síťových dat a sadu Jupyter notebooků s implementací experimentů. Použití Jupyter notebooků pro datovou analýzu je dnes standardem. Vytknul bych nedostatek komentářů a vizualizací výsledků.

4. Hodnocení výsledků, jejich využitelnost 85 /100 (B)

Práce přináší novou metodu pro detekci TeamViewer aplikace pomocí statistických vlastností jeho provozu. Metoda byla ověřena na rozsáhlé datové sadě a dle dosažených výsledků se zdá být vhodná pro využití v praxi.

Celkové hodnocení 82 /100 (B)

Písemná i praktická část práce jsou dobře zpracované. Student si detailně nastudoval chování TeamViewer aplikace a analyzoval její provoz pomocí standardních metod pro monitorování síťového provozu a pro následnou datovou analýzu. Celkově navrhuji hodnocení stupněm B.

Otázky k obhajobě

- Obsahuje PSTATS sekvence pakety s nulovou délkou (např. TCP ACK)? Pokud ano, jsou tyto pakety důležité pro klasifikaci?
- Jakým způsobem byly vybrány hyper-parametry jednotlivých modelů?
- V rámci práce vznikly dvě datové sady – neplánuje se jejich zveřejnění?

Instrukce

Splnění zadání

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.

Písemná část práce

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.

Nepísemná část, přílohy

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.

Hodnocení výsledků, jejich využitelnost

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.

Celkové hodnocení

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.