FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Karel Hynek
Student:	Bc. Radek Smejkal
Název práce:	Klasifikace komunikace SSH protokolu
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	19. 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 práce bylo splněno v celém rozsahu. Pro kvalitní a důvěryhodné otestování vytvořeného algoritmu se student rozhodl využít opravdová data ze sítě CESNET2, která ale nebyla anotovaná. Nad rámec zadání si tedy student dostudoval použití pokročilých algoritmů datové analýzy, které nejsou v rámci oboru bezpečnosti vyučovány. I tak se jednalo o velice obtížný úkol, který ale byl v rámci této práce výborně vyřešen.

2. Písemná část práce 95 / 100 (A)

Text práce je nadprůměrně rozsáhlý. Oceňuji podrobný popis zkoumaného protokolu SSH, který považuji za velice kvalitní. Text práce je celkově dobře členěný a dobře se čte. Všiml jsem si pouze drobných typografických nedostatků, nicméně žádné překlepy či gramatické chyby jsem nezaznamenal.

3. Nepísemná část, přílohy 90 / 100 (A)

Nepísemná část práce je poměrně bohatá. Obsahuje datovou sadu anotovanou a anonymizovaná a částečně i oštítkovaná data ze sítě CESNET2. Dále obsahuje jupyter notebooky, které byly používány pro datovou analýzu a návrh detekčního algoritmu. Tyto notebooky jsou poměrně čitelné a dobře strukturované. V neposlední řadě je přiložený hotový NEMEA modul napsaný v jazyce python. Ačkoliv je tento modul poměrně dobře okomentovaný, ocenil bych použití i nějakého automatického nástroje pro tvorbu dokumentace, jakými jsou například pydoc, či sphinx.

4. Hodnocení výsledků, jejich využitelnost 100 /100 (A)

Využitelnost výsledků je značná a to nejen v síti CESNET2. Student dokázal navrhnout velice přesné detekční algoritmy, které dokáží zjistit velké množství informací z šifrovaného SSH provozu, a tím zvýšit celkovou bezpečnost na síti bez závažného narušení soukromí uživatelů. Implementované algoritmy pomohou v sítích detekovat špatně nastavená pravidla pro přihlašování (například detekce přihlášení heslem), či útoky hrubou silou (pomocí detekce neúspěšného přihlášení).

5. Aktivita studenta

- [1] **výborná aktivita**
- [2] velmi dobrá aktivita
- [3] průměrná aktivita
- [4] slabší, ale ještě dostatečná aktivita
- [5] nedostatečná aktivita

Student se účastnil pravidelných konzultací a to i v době pandemie. Na konzultace byl vždy perfektně připraven.

6. Samostatnost studenta

- [1] **výborná samostatnost**
- [2] velmi dobrá samostatnost
- [3] průměrná samostatnost
- [4] slabší, ale ještě dostatečná samostatnost
- [5] nedostatečná samostatnost

Student uložené úkoly plnil samostatně a dokázal případné náměty vedoucího práce i dále rozvíjet.

Celkové hodnocení 95 /100 (A)

Celkově práci hodnotím velice vysoko a kladně. Student provedl pečlivou analýzu protokolu SSH a to nejen v rámci specifikace, ale i v rámci chování SSH protokolu na paketové úrovni. Tyto znalosti dokázal následně využít v návrhu algoritmu klasifikace SSH komunikace, který je implementován jako NEMEA modul. Pečlivé vyhodnocování přesnosti na reálných datech z páteřní sítě značným způsobem zvyšuje důvěryhodnost ve funkčnost a nasaditelnost takového algoritmu na reálné síti. Z výše popsaných důvodů hodnotím práci stupněm A.

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.

Aktivita studenta

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.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

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.