



Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Koumar
Student:	Dominik Oškera
Název práce:	Detekce botnetů pomocí periodického chování síťového provozu
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	27. května 2025

Hodnotící kritéria

1. Splnění zadání

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

Student plně splnil zadání a zejména vytvořením unikátní datové sady práce dalece přesahuje rozsah bakalářské práce. I přes to, že je zadání ambiciózní na bakalářskou práci, tak si s prací student skvěle poradil.

2. Písemná část práce

100/100 (A)

Text práce považuji za rozsahově lehce nadprůměrný, dobře strukturovaný a pochopitelný pro čtenáře. V práci jsem neobjevil žádné věcné nedostatky či nepravdy. Grafy a tabulky v práci jsou vhodně strukturované i velikostně přiměřené, jedinou nedokonalostí je, že občas tabulka lehce přesáhne okraj textu dle šablony. Nicméně dané tabulky by nešlo triviálně předělat, tak aby nepřesahovali text a zároveň ukazovali potřebné fenomény, proto to nepovažuji za chybu. Po citační stránce student citoval nejvíce relevantní vědecké publikace z domény monitorování síťového provozu a detekce hrozeb v přiměřeném počtu i kvalitě daných publikací. Další citace obsahují relevantní články z blogů, které obsahují nejnovější informace o botnetech. Citační etika porušena nebyla. Celkově je text velice povedený a proto uděluji 100 bodů.

3. Nepísemná část, přílohy

100/100 (A)

Přílohy práce obsahují kód metody pro získání featur pomocí mé metodologie využívající Lomb-Scargle periodogram. Je nutné poznamenat, že kód metody student celý reimplmentoval čímž pomohl reproducibilitě jak své vlastní práce, tak předchozích již

publikovaných prací. Kód je dobře strukturovaný, dokumentovaný a dodržuje coding style PEP8. Nemám vůči němu žádné námitky a proto hodnotím 100 body.

4. Hodnocení výsledků, jejich využitelnost

100/100 (A)

Tato práce vznikla za účelem ověření toho zda metoda klasifikace šifrovaného síťového provozu pomocí periodicity lze aplikovat na detekci botnetů. Student uchopil výzkum natolik dobře, že se podařilo nejen tuto myšlenku potvrdit na dvou datových sadách což samo osobě postačuje na významný přínos poznání v této doméně. Ale student navíc dokázal vytvořit novou datovou sadu, která má zatím unikátní parametry jelikož žádná datová sada zaměřená na detekci hrozeb nemá tak dlouhé záchyty botnetů a takový rozsah různých botnetů (32 různých binárek). Tento fakt je extrémně důležitý, jelikož v doméně detekce hrozeb v síťovém provozu se jedná o netriviální úkol a potřeba nových datových sad je momentálně často adresovaná jako otevřená výzva v řadě relevantních kvalitních publikací. Proto je v přípravě článek o tomto výzkumu, který bude odeslán do časopisu Computer Networks.

5. Aktivita studenta

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

Student byl naprůměrně aktivní během celé práce. Účastnil se dokonce i projektu VýLeT s tímto tématem. Každý týden se účastnil konzultací kde se aktivně podílel na plánování dalšího postupu. Vypracování této odevzdané práce se věnoval velmi svědomitě, řešení věnoval velké úsilí. Díky tomu se podařilo dosáhnout kvalitních výsledků, které mají do budoucna velký publikační potenciál.

6. Samostatnost studenta

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

Student samostatně prováděl naplánovaný výzkum a experimenty. Navíc vyvíjel nadprůměrnou iniciativu.

Celkové hodnocení

100/100 (A)

Zadání práce bylo splněno, odevzdané výsledky jsou rozsáhlé a ve vysoké kvalitě, čehož se podařilo dosáhnout díky studentově nadprůměrné aktivitě, iniciativě a samostatnosti. Vytvořené výsledky mají publikační potenciál a budou základem budoucí vědecké publikace.

Instrukce

Splnění zadání

Posudte, 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, posudte 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 posudte, 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. Posudte správnost používání formálních zápisů obsažených v práci. Posudte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posudte, 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 posudte, 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 posudte schopnost studenta samostatně 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.