FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Karel Hynek
Student:	Bc. Jakub Osmani
Název práce:	Detekce phishingových domén ve vysokorychlostním síťovém provozu
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	5. ledna 2024

Hodnotící kritéria

1. Splnění zadání

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

Zadání bylo splněno v plném rozsahu. Student navíc popsal výsledky vlastního výzkumu phishingových útoků v kapitole "Practical Dive into Phishing".

2. Písemná část práce 100 / 100 (A)

Text práce je psaný výbornou angličtinou a je dobře strukturovaný. Text postupně popisuje jednotlivé kroky, které student v rámci diplomové práce provedl a zároveň shrnuje i problémy a slepé cesty na které narazil. V rámci práce jsem zaregistroval pouze minimum překlepů a typografický chyb. Celkově se práce velmi dobře čte, je informačně bohatá a působí dobrým dojmem.

3. Nepísemná část, přílohy 95 / 100 (A)

Nepísemnou část práce považuji za velice kvalitní. Obsahuje zdrojové kódy v jazyce python a vytvořené datasety. Zdrojové kódy jsou dobře čitelné, nenašel jsem místo kde bych měl problém s pochopením. Navíc, zdrojové kódy jsou i přehledně komentovány. Jediným problémem je absence dokumentačních řetězců pro automatizované generátory dokumentace (jako je například sphynx).

4. Hodnocení výsledků, jejich využitelnost 95 / 100 (A)

Ačkoliv vytvořený systém není dokonalý a skládá se převážně z různorodých filtrů postupně selektující domény podezřelé na phishing, což má za následek, že většina

podezřelých domén jsou falešná pozitiva, považuji výsledky za dobré a užitečné. Vytvořený software běží v testovacím režimu na jednom z kolektorů sdružení CESNET s pomocí dalších indikátorů phishingu pomáhá hledat phishingové domény čímž zvyšuje celkovou bezpečnost uživatelů národní akademické sítě.

5. Aktivita studenta

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

Student byl velice aktivní a na pravidelné konzultace docházel vždy včas.

6. Samostatnost studenta

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

Student byl velice samostatný. Během práce přinášel vlastní nové nápady vedoucí ke zlepšení vytvořeného detektoru.

Celkové hodnocení 100 /100 (A)

Zadání práce ukládá studentovi obtížný úkol detekce phishingových domén bez možnosti analýzy přenášeného obsahu. Ačkoliv je tento úkol extrémně obtížný, domnívám se, že si s ním student výborně poradil a vytvořil systém různě přesných a různě rychlých filtrů, které umožňují provozování na vysokorychlostní síti a zároveň jsou dostatečně přesné. Student trávil velké množství času nad návrhem a experimentálně vyhodnocoval jednotlivé přístupy selekce domén podezřelých na phishing nad reálnými doménami ze sítě CESNET. Vytvořený prototyp je použitelný a již dokázal najít některé potvrzené phishingové domény cílící na uživatele české pošty. Text práce považuji za rovněž velice kvalitní a perfektně dokumentuje studentovo uvažování v průběhu návrhu detektoru. Z těchto důvodu doporučuji práci k obhajobě a hodnotím 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. 52/2021, 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.