FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Karel Hynek
Student:	Bc. Lukáš Melcher
Název práce:	Detekce skrytých kanálů používající DNS over TLS
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	26. května 2022

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 plném rozsahu. Student navíc nad rámec zadání provedl analýzu možnosti exfiltrace dat skrz několik běžně se používajících poskytovatelů DNS over TLS (DoT).

2. Písemná část práce

80 / 100 (B)

Text práce je logicky strukturovaný, během jeho čtení jsem nezaznamenal žádné překlepy. Pouze jsem našel drobné typografické chyby (předložky na konci řádků, přetékání textu, chybějící ukončení závorky a jiné). Oceňuji i citační styl, který jasně ukazuje, jaká informace je citována. Text práce ovšem často obsahuje obraty a výrazy — "nechť si čtenář povšimne", "není ideální", či "vyhodnocení výsledků bylo prosté" — které jsou pro technický a odborný text nezvyklé. Místy je popis experimentů hůře čitelný a jeho pochopení vyžaduje naprosté soustředění čtenáře. Celkově ale text hodnotím jako dobrý.

3. Nepísemná část, přílohy

75 / 100 (C)

Elektronická příloha obsahuje datové sady využité k analýze a návrhu detekčního algoritmu a python skript s implementovaným klasifikátorem. Ačkoliv je zdrojový kód psaný čitelně, chybí v něm dokumentační komentáře. Navíc obsahuje zbytečné řádky, které jsou zakomentované. U datových sad zas postrádám README, které by vysvětlilo, co je v každé datové sadě obsažené a k čemu byla použita. Dále nerozumím, proč přiložená elektronická příloha neobsahuje analytické jupyter notebooky, které sloužily k návrhu a testování implementovaných klasifikátorů.

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

Výsledky práce považuji za velice užitečné. Student otestoval několik možností detekce exfiltrace dat skrz šifrovaný DoT kanál. Nejpřesnější algoritmus, vytvořený pomocí strojového učení, byl následně implementován jako python skript, schopný zpracovávat reálná síťová data. Dále student nad rámec zadání experimentálně otestoval možnosti exfiltrace dat skrz několik poskytovatelů DoT. Výsledky těchto experimentů považuji za velice zajímavé a stanou se základem plánované konferenční publikace.

5. Aktivita studenta

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

Student byl v průběhu práce velice aktivní, na domluvené schůzky přicházel 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 na práci pracoval samostatně. Podněty vedoucího práce dále samostatně rozvíjel a vylepšoval.

Celkové hodnocení 85 /100 (B)

Samotné zadání práce je výzkumného charakteru, což se pojí se zvýšenou náročností a množstvím problémů, které musel student vyřešit. Jsem přesvědčen, že si se všemi problémy student obstojně poradil a práci považuji za zdařilou. V rámci práce se student nejprve seznámil s protokoly šifrovaného DNS, možnostmi a přístupy síťového monitoringu, strojovým učením a nastudoval si současné poznání v oblasti detekce skrytých kanálů využívající protokol DNS. Tyto informace následně využil během tvorby experimentů a návrhu klasifikačních algoritmů. Student implementoval několik algoritmů, jejichž přenost vyhodnocoval a porovnával. Následně naimplementoval prototyp ve formě python skriptu, který je schopen zpracovávat reálná síťová data a detekovat DoT exfiltraci s přesností přesahující 99%. Nad rámec zadáni byla otestována možnost exfiltrace skrz několik poskytovatelů DoT. Toto testování se stane základem budoucí publikace.
Výsledky práce jsou podle mého názoru nad míru užitečné a zajímavé, a proto ji doporučuji k obhajobě. Nicméně nedostatky v písemné a nepísemné části celkově snížily dojem, a proto hodnotím práci stupněm B.

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.