FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Karel Hynek
Student:	Anton Aheyeu
Název práce:	Automatická tvorba databáze TLS otisků
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	27. 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 bylo splněno v celém rozsahu.

2. Písemná část práce 75 /100 (C)

Text práce je psaný v angličtině, v průběhu jeho čtení jsem zaznamenal drobné překlepy a typografické chyby. Zřídka se v textu vyskytují neobratné formulace vět. Bakalářská práce cituje celkem 49 zdrojů, nicméně na některých místech mi reference vyloženě chyběly (například u popisu JA3 fingerprintu nebo u popisu osquery). Text je celkově dobře strukturovaný, jednoduše čitelný, dobře dokumentuje vytvořený software a zdůvodňuje návrhová rozhodnutí. Kapitola 4 - testování by si ale podle mého názoru zasloužila více prostoru a minimálně obrázek testovacího prostředí. V popisu také chybí informace ohledně použitých OS pro testování fingerprintingu, což znemožňuje vyhodnocení relevance provedených testů.

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

Nepísemná část se skládá ze zdrojových kódů vytvořeného softwaru. Jmenovitě se jedná o: rozšíření do exportéru ipfixprobe, skript pro vytváření databáze s TLS otisky a samotný fingerprinting NEMEA modul. Zdrojové kódy jsou perfektně dokumentované, čitelné a je na nich vidět studentova pečlivost.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Výsledek práce je podle mého názoru velice hodnotný. Rozšíření exportéru ipfixprobe dohromady s dalším skriptem umožňuje automaticky vytvářet a rozšiřovat databázi TLS otisků. Tato databáze je následně využívána NEMEA modulem pro fingerprinting, který je schopný zpracovávat reálná síťová data. Je důležité zmínit velký potenciál vytvořeného rozšíření exportéru ipfixprobe, který dokáže obohatit síťové toky o informace o operačním systému klienta a komunikujícím procesu. To lze využít i na tvorbu datových sad pro další problémy síťového monitoringu.
Nicméně nemohu dát plný počet bodů a to z důvodu nedostatečného vyhodnocení implementovaného modulu TLS fingerprintingu, které pro případné nasazení bude třeba ještě doplnit.

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, na konzultace vždy chodil včas a byl připraven.

6. Samostatnost studenta

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

Student dokázal problémy vzniklé v průběhu implementace samostatně řešit. Mé návrhy na řešení samostatně rozvíjel, vylepšoval a realizoval.

Celkové hodnocení 85 /100 (B)

Celkově považuji práci za zdařilou. Student se seznámil s možnostmi monitorování síťového provozu, s TLS fingerprintingem a se systémem osquery. Na základě teoretické části dokázal navrhnout a implementovat rozšíření exportéru síťových toků ipfixprobe. Dále vytvořil podpůrný software pro automatickou tvorbu databáze TLS otisků. Také implementoval NEMEA modul pro realizování TLS fingerprintingu. Vše následně otestoval. Popis testování ovšem považuji za velice slabý a celkově snižuje i využitelnost. Vzhledem k dalším nedostatkům v textové části hodnotím práci stupněm B a doporučuji ji k obhajobě.

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.