FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Tomáš Čejka, Ph.D.
Student:	Pavel Valach
Název práce:	Analýza a detekce WireGuard provozu
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	4. února 2024

Hodnotící kritéria

1. Splnění zadání

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

Odevzdaná práce obsahuje podrobnou analýzu protokolu WireGuard. Součástí je i implementace navržených metod pro detekci WireGuard provozu na síti a rozpoznání pravděpodobného typu přenášeného obsahu. Vyvinutá detekce na principu Deep Packet Inspection je součástí veřejně dostupného open source flow exportéru ipfixprobe. Práce dále prezentuje experimentální vyhodnocení detekce pomocí rozšířených IP toků a metod strojového učení.

2. Písemná část práce 90 /100 (A)

Práce obsahuje drobné typografické a jazykové nedostatky, které však nemají zásadní vliv na porozumění textu. Práce obsahuje dostatečné množství citovaných zdrojů, které jsou použity v souladu s citačními zvyklostmi. Práce je vypracována v angličtině a kvalita je celkově, podle mého názoru, na vysoké úrovni.

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

Výsledkem práce jsou primárně datové sady a zdrojové kódy softwarové implementace navrženého řešení. Dále vzniklo prostředí pro záchyt zájmového provozu pomocí virtuálních strojů, které jsou replikovatelné vytvořenými skripty. Experimenty s klasifikací síťového provozu pomocí modelů strojového učení byly realizovány pomocí Python notebooků a tudíž jsou rovněž snadno opakovatelné. Zdrojové kódy pro softwarový nástroj ipfixprobe byly po důkladném otestování začleněny do veřejného Github repozitáře a jsou součástí master větve pro stabilní verze nástroje.

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

Detekce komunikačních tunelů v síťovém provozu je z pohledu síťové bezpečnosti užitečná pro získávání přehledu o aktivitě v infrastruktuře, což zlepšuje situační povědomí. Rozšíření nástroje ipfixprobe o detekci WireGuard protokolu je funkční a produkčně se používá pro monitorování v reálných síťových infrastruktur. Detekční modely vyvinuté a otestované pomocí zachycených datových sad pomáhají zlepšit vhled do šifrovaného síťového provozu.

5. Aktivita studenta

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

Vezmeme-li v úvahu celkovou dobu studentova studia, byla aktivita při řešení bakalářské práce spíše průměrná a to kvůli rozložení v čase. Výsledkem jsou však kvalitní výstupy.

6. Samostatnost studenta

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

Studentova samostatnost byla vynikající a to především při detailním studiu protokolu WireGuard a při vývoji infrastruktury pro vytváření datových sad provozu tohoto protokolu. Návrh a realizace implementačních výsledků této práce jsou kvalitní a svědčí o studentově rozsáhlých praktických zkušenostech z oblasti budování a správy produkčních systémů a infrastruktur.

Celkové hodnocení 95 /100 (A)

Písemná část práce sice obsahuje drobné nedostatky, ale celkově je odevzdaná práce na výborné úrovni. Výsledky jsou užitečné pro síťovou bezpečnost a monitorování síťového provozu. Vyvinuté rozšíření pro ipfixprobe bylo začleněno do stabilní veřejně dostupné verze tohoto nástroje.

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.