FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Martin Čtrnáctý
Vedoucí: práce:	Ing. Tomáš Čejka, Ph.D.
Název práce:	Softwarový modul pro rozpoznání VPN v síťovém provozu
Obor:	Počítačové systémy a sítě

Datum vytvoření: 7. 6. 2020

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
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.

Komentář:

Práce se zaměřuje na analýzu VPN provozu a jeho identifikaci na paketové a tokové úrovni. V rámci práce vznikly datové sady, detailní analýza chování protokolu OpenVPN a Cisco AnyConnect a nakonec i návrh a implementace detekčních algoritmů pro rozpoznání VPN provozu. Odevzdaná práce splňuje všechny body zadání.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*75 (C)*

Popis kritéria:
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. 26/2017, 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.

Komentář:

Písemná část práce splňuje standardní rozsah diplomových prací, obsahuje všechny potřebné informace. Struktura textu by se dala vylepšit, především informace v kapitolách o Analýze a Testování působí nepřehledně a bylo by vhodnější text trochu přeskládat.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*90 (A)*

Popis kritéria:
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

Komentář:

Klíčové pro řešení tohoto tématu bylo vytvoření dostatečně velké datové sady obsahující vzorky VPN komunikace. Student během své práce datové sady nasbíral pro různé konfigurace VPN nástrojů. Na základě analýzy provozu bylo navrženo a implementováno celkem pět různých detekčních metod založených na paketové nebo tokové analýze. Tyto prototypy detektorů bylo potřeba vytvořit kvůli důkladnému vyhodnocení a porovnání různých algoritmů klasifikace OpenVPN, Cisco AnyConnect a obecného VPN spojení.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*89 (B)*

Popis kritéria:
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.

Komentář:

Téma práce se týká významné výzkumné oblasti analýzy šifrovaného provozu. Cílem bylo rozpoznat VPN spojení v normálním provozu. Důvodem je detekce potenciálně nepovoleného šifrovaného provozu, jež může obsahovat např. citlivá data, která chce útočník přenést vně organizace. Podle výsledků prezentovaných v diplomové práci se zdá, že vyvinuté a testované metody fungují dobře. Před nasazením v praxi však bude potřeba testy ještě rozšířit.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: *1=výborná aktivita,* ***2=velmi dobrá aktivita,*** *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 5b: *1=výborná samostatnost,* ***2=velmi dobrá samostatnost,*** *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
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 (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student pracoval samostatně a aktivně po celou práce, účastnil se pravidelných konzultací, na které byl dobře připraven.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*89 (B)*

Popis kritéria:
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.

Text hodnocení:

Odevzdaná diplomová práce se zabývá náročnou problematikou analýzy šifrovaného provozu a rozpoznání konkrétního typu komunikace generované VPN aplikacemi. V rámci práce vznikly datové sady a pět různých detekčních algoritmů zaměřených na rozpoznání VPN komunikace. Práce má velký potenciál pro bezpečnostní analýzu a po rozšíření testů a provedení dalších experimentů má i publikační potenciál.

Podpis vedoucího práce: