FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Pavel Šiška
Vedoucí: práce:	Ing. Tomáš Čejka, Ph.D.
Název práce:	Adaptivní mitigace DDoS útoků na základě online analýzy
Obor:	Počítačová bezpečnost

Datum vytvoření: 20. 1. 2021

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 zabývá analýzou problematikou zpracování paketů z vysokorychlostní linky v online režimu. Cílem práce bylo vytvořit softwarový prototyp nástroje, který pomocí analýzy zjistí strukturu síťového provozu a najde pravidla umožňující mitigaci DDoS útoků. Téma bylo po teoretické i praktické stránce prozkoumáno a práce byla splněna.

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

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:

Odevzdaný text práce je v pořádku po věcné-obsahové i formální stránce. Práce je informačně bohatá a obsahuje všechny podstatné části.

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

Výsledkem práce je funkční softwarový prototyp nástroje, který umí zpracovat posloupnost paketů z vysokorychlostní linky a s dostatečnou rychlostí zpracování získat i) informace o struktuře analyzovaného provozu (tzn. zastoupení protokolů a zdrojů provozu) a ii) sadu pravidel, která popisují nejvíce zastoupený provoz pro systém obrany proti DDoS útokům. Vytvořený nástroj byl důkladně otestován a do budoucna je možné jej integrovat do systému DDoS mitigace vyvíjeného sdružením CESNET.

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

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:

Text práce popisuje motivaci tohoto tématu na reálném případu zahlcení monitorovací infrastruktury. Tato práce reaguje na popsanou situaci, kdy monitorovací sondy a kolektor nezvládají sbírat informace o nejvíce zastoupeném provozu. Výsledkem práce je vyvinutý softwarový nástroj, který může běžet na dedikovaném zařízení pro DDoS obranu, na které se v krizové situaci může přesměrovat provoz útoku. Díky tomu bude schopen mitigační systém autonomně identifikovat, který provoz je potřeba zahodit tak, aby se zajistila provozuschopnost infrastruktury. Vyvinutý prototyp navíc navrhuje pravidla, která může správce sítě rovnou aplikovat, což ušetří čas.

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 velice aktivně a samostatně po celou dobu své závěrečné práce. Tématu DDoS mitigace se student věnuje v podstatě celé studium, což mělo velice pozitivní vliv na kvalitu vytvořené práce. Student je navíc aktivním členem laboratoře monitorování síťového provozu, pro kterou je cenným přínosem.

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

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 práce je na výborné úrovni. Téma bylo důkladně zpracováno, v teoretické části byl proveden průzkum existujících použitelných technologií a na základě toho byl vytvořen návrh vhodného řešení. Vytvořeným výsledkem je kvalitní otestované inženýrské dílo, které může být použito v praxi.

Podpis vedoucího práce: