FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jiří Smítka
Student:	Lukáš Brůna
Název práce:	Moderní slow DDoS útoky a ochrana proti nim
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	11. června 2024

Hodnotící kritéria

1. Splnění zadání

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

bez výhrad

2. Písemná část práce 95 /100 (A)

Práce je napsána ve velmi čtivé a kvalitní angličtině. Formální stránku hodnotím obecně jako výbornou. Jednotlivé kapitoly na sebe navazují, student rozumně vyžíval a citoval zdroje informací. Ocenil jsem mimo jiné i výčet slepých cest, kterými se autor vydal a které k řešení nevedly. Možná bych doporučil doplnit do popisku k obrázku 2.2, na kterém není nic vidět, komentář, že na tomto obrázku není nic vidět a to je právě to, proč je tento obrázek tak zásadní. Kapitola 4 popisuje vývoj díla, avšak některé části textu by zasloužily přesun do části s analýzou. Moje námitky jsou však spíše bagatelní.

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

Autor při implementaci využil (v souladu s licencemi) cizí kódy (příklady na použití), přičemž se na použité zdroje vždy odkazuje. Výsledné dílo je sice celkem krátké, je však výsledkem mnohých autorových experimentů (z nichž by si mohl některé ušetřit, kdyby provedl hlubší analýzu - nutno však zdůraznit, že někdy je rychlejší provést malý pokus, než dlouze hledat v dostupných zdrojích informace).

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

Práce je velmi nadějná, má potenciál pro použití v praxi. Dílo však nebylo nijak rozsáhle testováno, zejména s jinými anti-DDoS nástroji. Zajímavé je, že autor postavil dílo na

detekci nulové hodnoty TCP okénka, což vypadá na celkem originální myšlenku. Asi by to chtělo rozšířit analýzu o hlubší vyhledání nástrojů, které tuto techniku používají (jsou-li).

Celkové hodnocení

95 /100 (A)

Bakalářská práce se mi líbila. Dílo má potenciál na další rozvoj.

Otázky k obhajobě

1) Dohledal jse na Internetu jiné nástroje, které by detekovaly SDDoS útok stejnou technikou jako Vy? Můžete se k nim nějak vymezit?
2) Nijak jste v práci nezmínil možnost řešit analýzu TCP hlaviček přímo v jádře linuxu. Zamyslete se, kde by se analýza prováděla a jak by detekce mohla fungovat. Porovnejte toto řešení s Vaším stávajícím dílem.

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.

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.