FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Jan Fesl, Ph.D.
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

Předložená bakalářská práce obsahuje veškeré dílčí cíle, které byly zmíněny v zadávacím protokolu bakalářské práce.

2. Písemná část práce 60 / 100 (D)

Kvalita písemné části práce je proměnlivá, resp. částečně se postupně zhoršuje. V úvodní části, která se věnuje principům Slow DDOS útoků, je práce kvalitní a relativně podrobná, naopak popis implementační části již tak podrobný není. Např. kapitola 3 postrádá úvod, který by zajistil kompaktnost práce, ve smyslu napojení na předchozí části. V kapitole 4 autor popisuje návrh a implementaci modulu, který je schopen zabránit jednomu typu DDOS útoku, který neprobíhá na úrovni aplikační vrstvy modelu OSI/ISO, tudíž webový server jej z prostřednictvím modulu zcela jednoduše vyřešit nemůže. Autor však navrhl alternativní řešení založené na spolupráci webserveru a proxy serveru, což hodnotím kladně. Autor bohužel v práci neuvedl důvody, byť mi je ústně sděloval, proč vytvářel řešení eliminující pouze jediný útok. V úvodu kapitoly 5 autor opět opomněl úvod, samotné testování přináší zajímavé výsledky. Nutno podotknout, že práce je psána srozumitelnou angličtinou, což celkově můj dojem z práce zlepšuje.

3. Nepísemná část, přílohy 80 / 100 (B)

Autor zhotovil několik skriptů v kvalitě odpovídající řešení proof-of-concept, které je pro daný typ práce odpovídající, nicméně modul pro webserver Apache není připravený pro produkční prostředí.

4. Hodnocení výsledků, jejich využitelnost 80 /100 (B)

Autor došel k zajímavým poznatkům zejména v oblasti programování modulů pro webserver Apache a k tomu, že určité typy slow DDOS útoků nejsou pro Apache použitelné již v základním nastavení. Autor navrh i elimninace útoku neprobíhajícím na aplikační vrstvě. modelu ISO/OSI. Informace o nemožnosti určitých slow DDOS útoků bohužel autor v práci explicitně nezmiňuje.

5. Aktivita studenta

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

Studentova aktivita byla zpočátku výborná, později se však ukázalo, že určité části práce (zejména kapitoly 4 a 5) byly podceněny, což způsobilo to, že práce byla dokončována pod časovým stresem. Celkově jsem však byl s aktivitou studenta spokojen.

6. Samostatnost studenta

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

Student se mnou práci konzultoval pravidelně, určité problémy dokázal vyřešit sám, jiné ve spolupráci se mnou.

Celkové hodnocení 75 /100 (C)

Autor vytvořil zajímavou práci, na které je zřejmé, že byla vytvářena pod časovým stresem s čím souvisí i její kvalita. Jak se v průběhu vytváření práce ukázalo, některé typy slow DDOS útoků funkční pro aktuální verzi webového serveru Apache nebyly již pro základní nastavení webového serveru, tudíž vytváření modulů vedoucí k eliminaci určitých typů slow DDOS útoků nebylo možné. Práci doporučuji 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.