FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš, Ph.D.
Student:	Lukáš Hrdonka
Název práce:	Detekce neautorizované komunikace moderními aplikačními firewally
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	26. května 2024

Hodnotící kritéria

1. Splnění zadání

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

2. Písemná část práce 80 /100 (B)

Písemná část práce pokrývá požadované oblasti a je po faktické stránce v pořádku, v tomto ohledu jsem spokojen. Kapitola 2.3 by mohla být podrobnější, s ohledem na už tak značnou délku práce v ostatních částech to ale není nezbytné. Menší výhrady mám k jazykové stránce textu, kdy vedle očekávatelných menších chyb v členech nebo čárkách narážíme příležitostně na obtížně srozumitelné formulace, které zhoršují čitelnost textu. Nejde však o tak častý nebo závažný problém, aby činil práci neupotřebitelnou.

3. Nepísemná část, přílohy 85 /100 (B)

Nepísemnou část práce tvoří zejména studentem vytvořené aplikace pro testování obou únikových technik, substituce i injekce. Tyto aplikace jsou jednoduché, ale svůj účel bez problémů plní. Mají jisté nedostatky z pohledu softwarového vývoje (dokumentace, nadbytečné převody mezi ANSI a Unicode, detekce konce síťových zpráv) i bezpečnosti (v inject.cpp může potenciálně přetéct buffer), ale protože jejich účel je jiný, nevnímám tyto chyby jako problém.

4. Hodnocení výsledků, jejich využitelnost 85 /100 (B)

Student ověřoval, jaká je aktuálně situace v oblasti možného úniku škodlivých aplikací z pozornosti aplikačního firewallu. Soudě dle výsledků se zdá, že moderní firewally toto

nebezpečí příliš neřeší, ale není jasné, proč vlastně. Důvodů může být více, i legitimních. Za zarážející považuji poměrně vlažnou odezvu ze strany vývojářů těchto nástrojů, je to pro mě varovné znamení. Uživatel práce by každopádně měl počítat s tím, že pokud už se nedůvěryhodný (nikoliv nutně škodlivý) kód dostane do jeho počítače, aplikační firewally mu spíše nezabrání v komunikaci s externím prostředím.

5. Aktivita studenta

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

6. Samostatnost studenta

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

Celkové hodnocení

85 /100 (B)

Student v rámci své bakalářské práce nastudoval problematiku aplikačních firewallů, seznámil se s některými možnostmi, jak může aplikace uniknout z jejich dosahu, a zkonstruoval dva typově velmi odlišné testy, kterým podrobil pět běžně používaných aplikačních firewallů. Výsledky nejsou příliš povzbudivé, testy vesměs dokázaly moderními firewally projít a komunikaci uskutečnit. To je poměrně zneklidňující. Celkové provedení práce považuji za velmi dobré a tomu odpovídá i výsledná známka.

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.