FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Yelena Trofimova, Ph.D.
Student:	Jan Lukáš
Název práce:	Botnets a útoky typu Distributed Denial-of-Service
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	13. června 2023

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

69 / 100 (D)

Práce má dobrou logickou strukturu. Vyskytují se drobné překlepy a chybějící čárky. Mám výhrady k použiti zdrojů: obě kapitoly 2 a 4 jsou celé převzaté z jednoho článku z roku 2011. Pak kapitola 3 je jiný článek z roku 2012, ale dokonce i názvy podkapitol odpovídají. U takového zadání bych čekala lepší rešerši více zdrojů a navíc, novějších. Aplikované protiopatření z experimentů nejsou navázané na kapitolu 4.
s.5 Figure 1.1: "Handlers" jsou pravděpodobně C&C servery, ale z popisu to není jasné.
Figure 2.1 a 4.1: Špatná kvalita obrázků.
Figure 5.2: chybí Presentation layer.
Table 5.1: zdroj? Navíc funkce Transportní a Sitové vrstev nejsou správně popsané.
s.27 Útok LAND byl problém pro Windows 2003 a XP, byl zveřejněný v roce 1997.
Table 5.2: SYN flood není bandwidth depletion, je to resource depletion.
Celá Kapitola 5: je to Transport, ne Transportation layer.
s.34-35: Teardrop byl reportovaný spolu s LAND v roce 1997. Bonk je z roku 2004.
s.39 Figure 6.1 Schéma sítě je matoucí, nepoužívá zavedené značení a navíc na schématu chybí připojeni každé stanice k Internetu. Ani na obrázku ani z textu není jasné, kde běží C&C server.
s.44 Bod 6. close() zavolaný na socketu zavírá spojení.

3. Nepísemná část, přílohy 75 /100 (C)

Student poskytl výsledky experimentu ve formě záznamu odchycených zpráv a logu vytíženosti serveru.

4. Hodnocení výsledků, jejich využitelnost 60 /100 (D)

Nemyslím se, že výsledky jsou využitelné v praxi.

Celkové hodnocení 70 /100 (C)

Vzhledem k výše uvedenému hodnotím stupněm C.

Otázky k obhajobě

1) BGP protokol má mechanizmy ke zmírnění DoS útoku (BGP flowspec). Do jaké kategorie podle Vaší klasifikaci patři?
2) Bylo by zajímavé experimentovat s platnými požadavky: jaké je chování napadeného serveru (bez/s protiopatřeními) z pohledu legitimního uživatele. Je pravděpodobné, že i legitimní požadavek by byl zahozen?

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.