FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jan Fesl, Ph.D.
Student:	Kamil Kopp
Název práce:	Zranitelnosti a útoky typu Distributed Denial-of-Service
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	4. června 2021

Hodnotící kritéria

1. Splnění zadání

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

Student zadání práce splnil, veškeré deklarované body byly dosaženy. Z hlediska obtížnosti lze obtížnost práce zařadit do v kategorie lehčí - průměrná.

2. Písemná část práce 70 / 100 (C)

Rozsahem a kvalitou práce je daná předložená práce standardní, dostačující požadavkům kladeným na bakalářské práce. Struktura práce je korektní, práci lze považovat za homogenní dobře srozumitelný celek. Po typografické, grafické, jazykové a citační stránce je práce rovněž na dobré úrovni. Vzhledem k detailnímu zaměření práce směrem k programu Memcached ovšem postrádám detailní rozbor parametrů tohoto programu, které jsou pro vytvoření útoku zásadní - tj. např. omezení max. počtu klientů, omezení počtu obsluhujících threadů, zapnutí autentizace přes SASL protokol, použití pouze TCP protokolu atd.

3. Nepísemná část, přílohy 70 / 100 (C)

Student vytvořil skutečně funkční řešení, které implementoval v prostředí virtuálních počítačů. Kvalita kódu implementace vytvořených skriptů resp. programu je dle mého názoru podprůměrná-průměrná např. na úrovni struktury kódu a použitých konstrukcí v BASH skriptech, část v C++ je pouze procedurální a ani nevyužívá žádné pokročilejší prvky jazyka C++. Provedené experimenty jsou plánovány logicky a dosažené výsledky jsou reprodukovatelné při znalosti nastavení parametrů programu Memcached a detailních podmínek měření.

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

Dosažené výsledky upozorňují na nedostatky programu Memcached, který je dnes poměrně rozšířeným aktuálním řešením. Vadou na kráse je ovšem to, jak již bylo předesláno, že autor, nevzal detailně v potaz samostatné interní možnosti nastavení parametrů programu eliminující možnost DDOS útoku - např. maxbytes, maxcons, threads atd. Bez prozkoumání použité konfigurace není jasné, jak lze dosáhnout obdobných výsledků. Navržené způsoby obrany jsou v obecné rovině správné, nicméně na zcela elementární úrovni. Co mi není úplně jasné, je to, proč generovaný síťový průtok vedený od jednoho útočníka přes jeden zranitelný server je vyšší než přes dva servery, toto autor ani nikterak nevysvětluje. Zabezpečení vůči tomuto útoku je dnes zřejmě snadné díky použití IDS/IPS systémů, jelikož mechanismus útoku se v principu od jiných DDOS útoků neliší.

Celkové hodnocení 75 /100 (C)

Práci doporučuji k obhajově.

Otázky k obhajobě

1) Pokoušel jste se experimentovat se změnou parametrů programu Memcached, které mohou ovlivnit možnost či intenzitu DDOS útoku.
2) V případě defaultní konfigurace, domníváte se, že daný DDOS útok je skutečně schopen narušit fungování běžné lokální sítě?

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. 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.

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.