FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš
Student:	Kamil Kopp
Název práce:	Zranitelnosti a útoky typu Distributed Denial-of-Service
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	26. května 2021

Hodnotící kritéria

1. Splnění zadání

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

Zadání práce bylo splněno. Student se musel vypořádat s tím, že původně zamýšlený útok NXNSAttack se nakonec nepodařilo zprovoznit a bylo tedy nutné v dosti pokročilé fázi realizace přejít na jiný moderní DDoS útok.

2. Písemná část práce 75 / 100 (C)

Textová část práce zasvěcuje čtenáře napřed do problematiky útoků typu DoS a následně do DDoS. Odtud přechází k popisu aplikace Memcached, vysvětlení, v čem spočívá její rizikovost a návrhu schématu pro demonstraci této zranitelnosti. Dále popisuje některé aspekty demonstrační implementace a zejména výsledná měření, která demonstrují velký útočný potenciál Memcached a tedy i velkou rizikovost jeho použití.

Text práce není věcně nesprávný, ale první dvě rešeršní kapitoly působí poněkud neuspořádaným dojmem. Zejména rozdělení DoS zranitelností do podkapitol 1.2, 1.3 a 1.4 není srozumitelné a zasloužilo by si detailnější vysvětlení. Zahrnutí Mirai botnetu do kapitoly o přetečení bufferu je pak vysloveně nešťastné, protože Mirai nemá s přetečením bufferu vůbec nic společného.

V některých místech má student chyby ve výpočtech, typicky o jeden bajt (např. str. 31, maximální velikost je 1048576 bajtů, z toho 1048516 bajtů tvoří užitečná data a 59 bajtů hlavička; dále obdobná chyba na str. 37).

Domnívám se, že výpočet celkového amplifikačního faktoru ve vyhodnocení by měl být doprovázen i teoretickým výpočtem maximálně dosažitelné hodnoty, založené na

vlastnostech protokolů IP a UDP; aktuálně je výpočet ovlivněn konkrétním nastavením použitého TCP/IP stacku.

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

Vytvořené kódy jsou poměrně jednoduché, což odpovídá tomu, že útok je velmi jednoduché provést. V některých částech by šlo použít i efektivnější řešení (např. memcached.cpp by klidně mohl vygenerovat payload sám na základě dalšího parametru), ale není pro to praktický důvod. Z pohledu čistoty kódu bych uvítal, kdyby student nekombinoval Cčkové a C++kové kódy a kdyby data z payload souboru četl binárně. U skriptů bych uvítal, kdyby klíčové údaje (adresa oběti apod.) byly vždy definovány jako proměnné na začátku skriptu, aby se daly snadno měnit.

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

Student připravil virtuální prostředí pro jednoduchou demonstraci DoS útoku pomocí Memcached. Při aktivaci prostředí jsem narazil na problémy při instalaci .ova archívu (končil na nesrozumitelných chybách, to ale mohlo být způsobeno rozdílem v použitých verzích VirtualBoxu) a připadá mi úplně zbytečné, aby byl uživatel nucen přenastavovat IP adresy ručně (proč toto nastavení není zahrnuto už přímo ve virtuálních strojích, nebo pokud to nejde, proč na to není připraven skript?). Jakmile ale virtuální stroje rozchodíme, je demonstrace útoku otázkou rozkliknutí jedné ikonky a problematika amplifikačního útoku je okamžitě zřejmá na zobrazených grafech. Jde tak o užitečný výukový nástroj.

5. Aktivita studenta

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

Student byl v rámci řešení práce spíše aktivnější, na kontrolní body byl připraven.

6. Samostatnost studenta

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

Samostatnost studenta byla nevyrovnaná. Některé situace zvládal samostatně s přehledem, některé už méně. Práci nakonec dokončil, takže v testu praxí obstál.

Celkové hodnocení 85 /100 (B)

Předložená bakalářská práce popisuje a demonstruje problematiku amplifikačních Denial of Service útoků. Není dokonalá, dílčí nedostatky jsou popsány výše, přesto jde podle mě o užitečný nástroj k vysvětlení, o čem tyto útoky jsou a co je činí tak

nepříjemnými. Přiložené virtuální prostředí umožňuje praktickou demonstraci teoreticky popsaných jevů. Bohužel se nepodařilo zprovoznit původně zamýšlený NXNS útok, na druhou stranu velmi kladně hodnotím, že student byl schopen operativně přejít na jiný typ útoku a zamýšlených cílů dosáhnout na něm. Celkově proto hodnotím práci B-velmi dobře.

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.

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.