FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	doc. RNDr. Ing. Petr Zemánek, CSc.
Student:	Jan Pánov
Název práce:	Studie zranitelností Linuxového jádra
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	24. srpna 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 splnil požadované zadání bakalářské práce. Detailně se seznámil s architekturou jádra operačního systému LINUX, s procesem vývoje systémových programů v OS LINUX a s několika typy zranitelností (vulnerability) OS LINUX. V hlavní části práce student úspěšně implementoval útok (exploit) proti vybrané zranitelnosti jádra OS (zranitelnost CVE-2019-9213).

2. Písemná část práce

75 / 100 (C)

Rozsah práce považuji za přiměřený. V části věnované zranitelnostem bych uvítal bohatší analýzu známých zranitelností systému LINUX (s více odkazy na literaturu). Dobré by bylo i uvést krátký historický přehled klasifikace významných typů zranitelností a způsobů jejich odstranění v systému. Po věcné stránce je práce v pořádku, práce má vhodnou logickou stavbu i návaznost jednotlivých kapitol. Práce je přehledně členěna a pro fundovaného čtenáře je dobře pochopitelná. Zdroje jsou správně a relevantně citovány, nedošlo k porušení citační etiky. Software použitý v práci je použit v souladu s licenčními podmínkami. V práci jsem nalezl několik drobných gramatických chyb (překlepů) - např. na str. 7 odst. 6 (fyziké místo fyzické), str. 13 nadpis (Analýya místo Analýza), str. 18 odst 1 ("zapsána da disk" místo "zapsána na disk"). Také by bylo vhodné v textu práce odlišit názvy souborů, proměnných, funkcí, ... od běžného textu jiným typem fontu - např. archiv initramfs (str. 3), funkce madvise() (str. 16), struktura cred (str. 25).

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

Program implementovaný studentem splňuje zadání práce - bylo ověřeno, že implementace exploitu vůči zranitelnosti CVE-2019-9213 je funkční. Nástroje použité pro implementaci jsou vhodné. Je třeba zdůraznit, že proces vývoje programů (modulů) jádra OS je velmi složitý a náročný, a že student (užitečně) strávil relativně mnoho času nutným studiem detailů vývoje modulů jádra OS LINUX.

4. Hodnocení výsledků, jejich využitelnost 70 /100 (C)

Práce přináší nový poznatek - ukazuje konkrétní případ možného závažného narušení bezpečnosti OS LINUX (a také aplikací běžících v prostředí OS LINUX).

Celkové hodnocení 75 /100 (C)

Na této práci je nutné ocenit nejen samotný výsledek (funkční program splňující zadání práce), ale i rešeršní činnost studenta (úvodní kapitoly práce) a také (a to zejména) znalosti, které student získal během procesu implementace modulu jádra OS LINUX. Zde je vhodné zmínit rčení "i cesta může být cíl". Celkově navrhuji hodnocení "C".

Otázky k obhajobě

Jaké byly největší překážky v procesu implementace? Která fáze byla nejnáročnější? Jaké vývojové nástroje jste použil a jaké jste uvažoval použít ale nepoužil?

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.