FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Michal Bambuch
Vedoucí: práce: Ing. Josef Kokeš
Název práce: Přetečení bufferu na haldě
Obor: Bezpečnost a informační technologie

Datum vytvoření: 27. 5. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
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.

Komentář:

Práce se zaměřuje na rešerši a implementaci známých útoků na haldu v knihovně glibc. Student nastudoval klasické útoky na unlink makro, double-free a use-after-free, poté novější návrhy pěti útoků z článku Malloc Maleficarum a nakonec také na nejnovější útok House of Einherjar. Ke čtyřem z těchto útoků také připravil funkční demonstraci, což významně překračuje moje očekávání ze zadání.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*98 (A)*

Popis kritéria:
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.

Komentář:

Textová část práce popisuje obecně problematiku přetečení bufferu, včetně typických příčin tohoto jevu v C/C++. Následně popisuje strukturu haldy v glibc, na kterou pak navazuje detailní popis jednotlivých známých útoků, jejich příčin, způsobů exploitace a dostupných oprav. V poslední kapitole jsou pak připraveny podklady pro úspěšné provedení čtyř útoků na haldu.

Text je velmi dobře čitelný, logicky členěný a téměř bez jazykových chyb (zaznamenal jsem dvě). Vše je výborně ozdrojováno, a to až na úroveň jednotlivých řádek ve zdrojových souborech knihovny, které jsou za tu kterou zranitelnost zodpovědné.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*98 (A)*

Popis kritéria:
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

Komentář:

Součástí práce jsou zdrojové kódy jednotlivých útoků a hlavně připravené virtuální prostředí, ve kterém je možné všechny útoky použít. Pro každý útok jsou připraveny nutné binární soubory (mnohdy zkompilované na jiné distribuci, která je však vždy přesně označena a je pro ni připraven návod na sestavení binárky) a návod, jak je spustit. Všechny útoky v připraveném prostředí správně fungují. Přitom je jejich použití nesmírně jednoduché, pro každý je připraven Makefile s konzistentní strukturou.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

4. Hodnocení výsledků, jejich využitelnost	*98 (A)*

Popis kritéria:
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.

Komentář:

Výsledkem práce je detailní popis a působivá demonstrace problematiky přetečení bufferu na haldě. Zájemci se zde seznámí s příčinami i následky zranitelností a mají možnost si velmi jednoduše vyzkoušet, jak tyto zranitelnosti fungují. Za zvlášť významné považuji též zdokumentování, ve které verzi knihovny glibc byl každý jednotlivý útok zablokován (pokud byl vůbec někdy zablokován), a to až na úroveň příslušných řádků kódu knihovny. Velmi také chválím přehledné tabulky se strukturou exploitu pro všechny implementované útoky. Vzniká tak komplexní, ucelené dílo provádějící čtenáře velmi důležitou oblastí bezpečného programování.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: *1=výborná aktivita,* *2=velmi dobrá aktivita,* ***3=průměrná aktivita,*** *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 5b: *1=výborná samostatnost,* ***2=velmi dobrá samostatnost,*** *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
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 (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student pracoval převážně samostatně, ale ve vhodných intervalech konzultoval a na tyto konzultace byl vždy výborně připraven.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*95 (A)*

Popis kritéria:
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.

Text hodnocení:

Student vypracoval vynikající práci. Nastudoval dostupné útoky na implementaci haldy glibc, detailně je popsal a připravil na většinu z nich praktickou demonstraci. To celé zachytil v jazykově téměř bezchybném textu a ve vysoce uživatelsky přívětivém virtuálním stroji pro praktické vyzkoušení. Práce si určitě zaslouží zvážit k doporučení na cenu děkana. Doporučuji k obhajobě a hodnotím A-výborně.

Podpis vedoucího práce: