FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Jakub Čudka
Vedoucí: práce:	Ing. Filip Štěpánek
Název práce:	Injekce kódu ve virtuálním prostředí pro operační systém Linux
Obor:	Počítačová bezpečnost

Datum vytvoření: 7. 6. 2020

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:

Zadání bylo splněno. Výstupem je funkční simulace útoku pomocí DMA, která je aplikovatelná i na fyzický HW (viz bod 4). Výhrady mám přážně k textové části (viz bod 2).

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*60 (D)*

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:

Text byl psán ve spěchu a vyžaduje stylistickou korektůru -- ve stavající formě se v něm vyskytují překlepy, hovorové obraty a typografické nedostatky (například na straně 47 v sekci 3.1 je špatně uveden odkaz na předchozí část textu).
Obsahově k realizaci výhrady nemám. Ovšem neznalý čtenář může mít problémy s pochopením pozice útočníka, kde student popisuje, jak vypadá použité virtuální prostředí, ale chybí jednoduchý popis (ilustrace), jak daný útok bude proveden. V analytické části jsou popsány mechanismy, které operační systém používá ke správě procesů a operační paměti, ovšem na tyto mechanismy je odkazováno v rámci návrhu a realizace útoku v minimální míře. Co mi v analytické části převážně chybí je podrobnější popis použitého Volatility frameworku (sekce 1.7, strana 29). Stávajicí popis považuji za stručný a není z něj jasné, jakým způsobem framework analyzuje operační paměť či jak analýza souvisí s profilem operačního systému. Jelikož se student často odkazuje na práci s nástrojem "linux_volshell", zasloužil by tento příkaz v části 1.7 daleko podrobnější popis, aby čtenář měl lepší představu o jeho architektuře a možnostech.
Na druhou stranu i přes zmíněné nedostatky bych zde chtěl zmínit sekce 2.2.1-2.2.3 popisující práci se škodlivým kódem, které mi přišly velmi zdařené a zajímavé.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*70 (C)*

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:

V textu ZP schází manuál. Výstup práce jsem testoval ve svém prostředí (viz bod 4) a i když jsem měl potíže výsledný skript spustit, nakonec jsem byl úspěšný s pomocí postupu pospsaném v kapitole realizace.

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

4. Hodnocení výsledků, jejich využitelnost	*80 (B)*

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:

Výstupem ZP jsou 2 Python skripty. První připravuje škodlivý kód (tzv. "reverse shell" pro útočníka) a druhý jej injektuje do obrazu operační paměti virtuálního stroje s OS Linux. Skript cílí na předem známý process, který útočník zná a měl možnost jej předem analyzovat (rámci ZP se jedná o nekončící smyčku). V rámci analýzy frameworkem Volatility je proces identifikován a následně upravován (nástrojem linux_volshell) s pomocí obrazu operační paměti. Škodlivý kód je injektován do procesu, procesu jsou následně (omezená) práva změněna na administrátorská a útočník získává vzdáleně přístup do virtualního stroje / stroje oběti (reverse shell).
Výstup jsem vyzkoušel na svém virtuálním prostředí s plnou úspěšností. Jelikož ZP simuluje útok, při němž má útočník přístup k DMA, vyzkoušel jsem nad rámec zadání výstup aplikovat na reálném HW -- útok byl úspěšný ve smyslu získání reverse shell, ovšem eskalace práv se nezdařila. Tento nezdar dávám za vinu práci s živým systémem a nezahrnuji ho do svého hodnocení.

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 samostatně a průběžně mě informoval o svém počínání. Pravděpodobně však z důvododu implementačních potíží odložil psaní textu na poslední chvíli a, bohužel, to je negativně znát na kvalitě textové části, ke které jsem se nemohl včas a v plné míře před odevzdáním vyjádřit .

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*75 (C)*

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:

ZP si kladla za cíl simulovat útok pomocí DMA -- tedy s přímým přístupem do operační paměti. Cílený útok na operační systém Linux lze úspěšně simulovat ve virtuálním prostředí pomocí výsledných Python skriptů vytvořených studentem. Skripty cílí na injektování škodlivého kódu do procesu uloženého v operační paměti, po jejichž aplikaci je útočníkovi zpřístupněn reverse shell s administrátorskými právy. Útok je plně funkční ve virtuálním prostředí a nad rámec zadání ZP jsem jej úspěšně vyzkoušel na reálném HW (ovšem bez eskalace administrátorských práv viz bod 4). Výsledky o aplikovaném útoku na HW jsem předal studentovi k obhajobě.
I když jsem s výsledky práce spokojen, své hodnocení zakládám převážně na textu ZP, který byl psán ve spěchu. Jak jsem popsal již v bodě 2, vyskytují se zde stylistické nedostatky a některé pasáže (např. funkce frameworku Volatility) by bylo potřeba popsat víc podrobně. Čtenář neznalý problematiky může mít problémy s pochopením zvoleného postupu.

ZP hodnotím stupněm C a doporučuji k obhajobě.

Podpis vedoucího práce: