Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Bc. Tomáš Hradský
Vedoucí práce: Ing. Petr Kurtin
Název práce: Skrývání virtuálního prostředí před malwarem
Obor: Počítačová bezpečnost

Datum vytvoření: 4. 6. 2017

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	***1=mimořádně náročné zadání,*** *2=náročnější zadání, 3=průměrně náročné zadání, 4=lehčí, ale ještě dostatečně náročné zadání, 5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Diplomová práce Bc. Tomáše Hradského se zabývá problematikou skrývání virtuálního prostředí nástroje VirtualBox, které detekují počítačové viry v průběhu analýzy v antivirových firmách. V dnešní době, kdy se každý den objevují desetitisíce nových počítačových virů, je část jejich analýzy prováděna automatizovaně i s pomocí virtuálních prostředí. Studované téma je velmi aktuální a z pohledu antivirových firem relevantní.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. 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 splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Předkládaná práce splňuje zadání diplomové práce.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami, 3=splňuje požadavky s většími výhradami, 4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Předkládaná práce splňuje rozsah kladený na diplomové práce.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*90 (A)*

Popis kritéria:
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.

Komentář:
Studované téma je strukturováno do osmi kapitol na 66 číslovaných stranách. Na úvod, kde je vymezeno téma a cíl práce, navazuje teoretická část práce, která ve svých třech kapitolách seznámí čtenáře s důvody vzniku počítačové virtualizace, její výhody a také podrobně popisuje hardwarovou podporu virtualizace v procesorech Intel. Praktická část se skládá z pěti kapitol, v nichž autor, kromě představení všech využitých pracovních nástrojů, podrobně rozebírá 13 oblastí, které mohou počítačové viry využít k detekci virtualizovaného prostředí, navrhuje a implementuje kód přímo pro VirtualBox, který tomu zabrání. Oceňuji, že jednotlivé oblasti byly různorodě zvoleny: týkající se jak jádra systému Windows a hardwarových ovladačů, tak i ze samotné hardwarové virtualizační podpory v procesorech Intel. Poslední kapitolou je závěr, kde jsou shrnuty výsledky.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*86 (B)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.

Komentář:
Diplomová práce splňuje všechny formální náležitosti pro závěrečné práce, ač s několika drobnými nedostatky: autor textu používá zbytečně mnoho podkapitol, navíc se shodným názvem a to „Skrývání“ (použito 13x), což má za následek, že na straně 60 – 61 se nachází třeba 6 podkapitol. Názvy použitých programů nejsou uvedeny v plném znění, ale jsou uvedeny jako zkratky (např. DbgView, WinDbg nebo ProcExp). Většina textu je řádně formátována, pouze místy je použito větší odřádkování (např. strana 11). Jazyková stránka práce má nedostatky v používání příliš hovorových výrazů (např. kapitoly 5.2.1, 5.3, 5.4), které nejsou vhodné pro odborný text.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*94 (A)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Autor prostudoval značné množství literatury, kterou řádně cituje. Citace obsahují pouze drobné chyby ve formátování a to v zarovnání textu (např. [2], [11], [13]), jinak jsou z faktického hlediska správné.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*91 (A)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Analýza jednotlivých detekčních metod virtualizačního prostředí je vždy detailně popsána i s ukázkami zdrojového souboru a řádně okomentována. Při popisu těchto detekcí občas autor opomíjel teoretickou část problematiky a pro čtenáře může být tak složité se v některých částech textu orientovat (např. používání konkrétních VMX intrukcí bez předchozího vysvětlení, viz strana 18).

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Převážná část výsledků z diplomové práce byla implementována do interní verze programu VirtualBox ve firmě Avast Software, která jej používá na svých serverech k analyzování počítačových virů.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 9b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:
Jako vedoucí práce musím poznamenat, že autor pracoval velmi samostatně, prostudoval značné množství literatury a dokázal se v tak komplexním tématu orientovat.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*92 (A)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Předkládaná práce Bc. Tomáše Hradského splňuje všechny požadavky kladené na diplomové práce. Práce ma logickou strukturu, text je i přes drobné nedostatky srozumitelný a čtivý, vybrané téma je nepochybně relavantní a výsledky z praktické části byly úspěšně použity v praxi. I přes složitost tématu, byl autor schopen dosáhnout cíle práce s dobrými výsledky. Diplomovou práci Bc. Tomáše Hradského doporučuji k obhajobě.

Podpis vedoucího práce: