FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student: Pavlína Kopecká
Oponent práce: Ing. Jiří Buček
Název práce: Aplikace pro zakódování škodlivého kódu
Obor: Bezpečnost a informační technologie

Datum vytvoření: 15. 6. 2018

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:
Zadání je náročnější, vyžaduje detailní porozumění nízkoúrovňového programování a kombinace znalostí z oblasti antivirových programů, assembleru a bezpečnostních exploitů.

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:
Studentka splnila zadání částečně, nerealizovala část enkodéru metodou "Shikata-ga-nai".

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:
Rozsah písemné zprávy je přiměřený.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*70 (C)*

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:
Práce obsahuje užitečný základní přehled o kódování škodlivého kódu za účelem jeho ztížené detekce a případně snadnějším průchodem sanitizací (testem na alfanumerické znaky).

Některé části práce jsou však málo srozumitelné. Problematika kolem GetPC a dekodéru není pořádně vysvětlena. Práce by si zasloužila podrobnější rozbor procesu dekódování včetně použití instrukcí, které jsou přímo vykonávané procesorem a přitom jejich strojový kód má podobu alfanumerických znaků.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*70 (C)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Komentář:
Studentka místy používá příliš vágní odkazy na zdroje i části své vlastní práce. Není dobré odkazovat na zdroj slovem "zde", "odtud". Popisky ukázek kódu na str. 36 a 37 jsou informačně chudé. Práce i se nevyhnulo menší množství překlepů a typografických chyb, např. předložky "s" na konci řádku.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*80 (B)*

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:
Až na výše zmíněnou nevhodnou formu odkazování pomocí "zde" jsem nenašel závažnější nedostatky.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*55 (E)*

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:
Výsledkem práce je jednoduchý program, který umožňuje zakódování vloženého shellkódu alfanumerickým enkodérem. To není nic principiálně nového, studentka však navrhla optimalizaci spočívající v efektivnějším vyhledání kódu z množiny alfanumerických znaků.

Testování s antivirovými programy bylo neprůkazné, jelikož první škodlivý kód se nepodařilo úspěšně zakódovat, a druhý škodlivý kód nebyl detekován ani v původní podobě. Studentka ani nepíše přesnou verzi virových definic, se kterými antivirus pracoval. Například na mém počítači Windows Defender oba přiložené soubory se škodlivým kódem odstraní (nezakódovaný i zakódovaný).

Ve vytvořeném programu "encoder.py" není uveden autor. Jsou však uvedeny odkazy na převzaté části (zejména GetPC a dekodér).

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:
Textová část práce poskytuje základní přehled o problematice kódování škodlivého kódu. Pro praktickou využitelnost vytvořeného programu by bylo potřeba ještě dost práce.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
Co byste musela udělat, aby šlo výstup Vašeho programu otestovat i na novějších systémech, než Windows XP?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*60 (D)*

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:
Studentka měla poměrně náročné zadání, proto i jeho částečné splnění je dostatečné. Vzhledem k výše uvedeným nedostatkům v textové i praktické části práce navrhuji hodnocení D.

Podpis oponenta práce: