FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Pavlína Kopecká
Vedoucí: práce:	Ing. Filip Štěpánek
Název práce:	Aplikace pro zakódování škodlivého kódu
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 12. 6. 2018

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:

Zadaní hodnotím jako náročné z důvodu nastudování si složitější problematiky úniku detekce antivirovým SW. Toto zadání bylo splněno, ovšem s výhradami k implementační části. Ačkoliv je analytická část vysvětlena i lajckému čtenáři, výsledná aplikace ještě vyžaduje vyšší stupeň ladění (viz bod 3). Další výtku mám též k absenci implementace enkodéru metodou Shikata-ga-nai, ovšem přihlížím k zmíněné náročnosti zadání.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*85 (B)*

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 ZP splňuje požadavky na bakalářskou ZP. Studentka analyzuje problematiku detekování škodlivého kódu a metody úniku této detekce. Je zde i část pojednávající o současných řešeních, se kterými je výsledná aplikace porovnávána. Návrh (konkrétně alfanumerického enkodéru) je pak založen na principech popsaných v analytické části. Metoda Shikata-ga-nai je zmíněna pouze teoreticky. Samotná realizace a testování aplikace je popsána za použití virtuálního stroje. Kapitola testování by zasloužila podrobnější popis testování a užití větší množiny škodlivých kódů.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*60 (D)*

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:

Výslednou aplikaci jsem si vyzkoušel ve virtuálním prostředí, kde jsem na instalaci Windows XP aplikoval škodlivé aplikace pomocí šablony poskytnuté studentkou. Škodlivý kód jsem generoval a zakódovával pomocí nástroje Metasploit (též popisovaném v textu v rámci analytické části) a následně pro porovnání vytvořil škodlivý kód pomocí nástroje Metasploit a zakódovával jej aplikací, která vznikla v rámci této práce. Další krok pak byl v analýze detekce pomocí antivirového softwaru Avast Free. Zde jsem zjistil, že aplikace má problémy se souborovými vstupy a výstupy, kde aplikace nerespektuje kódování vstupu a výstupu zadaném uživatelem. Zdrojový kód je však čitelný a komentovaný, tedy lze ho snadno opravit. Nicméně další testování jsem prováděl na neupraveném kódu a pouze přes ruční zadávání vstupu. Zkoušel jsem celkem 3 škodlivé kódy, kde 2 měly za cíl získat vzdálený přístup a 1 měl vytvvořit administrátorský účet. Pokusy o vzdálený přístup úspěšné nebyly -- kód pro reverse shell není funční ani pokud je zakódován pomocí nástroje Metasploit -- funguje pouze v nezakódované formě a tato skutečnost je též popsaná v textu. Zkusil jsem tedy kód pro tzv. bind shell a ten zakódovatelný i spustitelný pomocí referenčních nástojů byl, ovšem pomocí výsledné aplikace nikoliv. Můj poslední pokus o vytvoření administrátorského účtu úspěšný byl (poznámka -- jedná se o odlišný škodlivý kód než který byl užit v rámci ZP). Tedy mohu říci, že aplikace je pro některé druhy škodlivých kódů funkční, ovšem ze svých zkušeností usuzuji, že aplikace potřebuje ještě otestovat/odladit a zanalyzovat její chování na vícero druzích škodlivých kódů.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*75 (C)*

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 práce je aplikace pro příkazovou řádku zakódovávající škodlivý kód alfanumerickým enkodérem. Tato aplikace předpokládá na vstupu škodlivý kód v hexadecimálním tvaru pro prostředí Windows XP a na výstupu vypisuje škodlivý kód v zakódované formě. Tento kód pak uživatel využije při kompilaci škodlivé aplikace -- aplikace realizovaná v rámci této práce kompilaci neprovádí, jejím výstupem je škodlivý kód určený pro další zpracování. Výsledná aplikace však ještě vyžaduje vyšší stupeň ladění (viz komentář k bodu 3).

Implementace enkodéru metodou Shikata-ga-nai není přítomna.

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:

Studentka pracovala samostatně a pravidelně se zúčastňovala konzultací. Ovšem problémy týkající se řešení práce nediskutovala okamžitě při jejich odhalení, což mělo za následek negativní dopad na řešení (viz bod 3).

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*78 (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:

Výsledek ZP je funční, ale vyžaduje vyšší stupeň ladění a testování. I když mám výtky k textu (konkrétně kapitola testování v bodě 2 a fungování aplikace v bodě 3), tak práci považuji za první krok k pochopení netriviální problematiky škodlivých kódů, jejíž text je čtivý a dokáže neznajícímu čtenáři nabídnout úvod do tématu. Vzhledem k výše uvedenému hodnotím práci stupněm C -- 78 bodů.

Podpis vedoucího práce: