FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Vít Souček
Vedoucí: práce: Ing. Filip Štěpánek
Název práce: Aplikace využívající zranitelnost Dirty Cow pro operační systém Android
Obor: Bezpečnost a informační technologie

Datum vytvoření: 5. 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:
Zadání bylo splněno, výsledkem je aplikace pro operační systém Android, která obsahuje škodlivý kód, který využívá zranitelnosti "Dirty Cow" a umožní vzdálený přístup útočníkovi.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*100 (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:
ZP splňuje požadavky na bakalářskou ZP. Student důsledně analyzuje princip útoku pomocí CVE-2016-5195 neboli "Dirty Cow" a jeho návaznost na vláknové operace v operačním systému Android. Zde student šel do hloubky operačního systému Linux z důvodu vysvětlení postupu útoku a navržení samotné aplikace. Tyto kroky jsou dostatečně v textu popsány a jednotlivé postupy jsou navzájem odkazovány mezi kapitolami analýza/návrh/realizace.

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

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*100 (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 je aplikace pro operační systém Android, která obsahuje škodlivý kód umožňující vzdálenému útočníkovi přístup do zařízení oběti. Aplikace byla úspěšně otestována ve virtuálním prostředí -- konkrétně na architektuře x86-64. Práci lze rozšířit -- prostor vidím v 32-bitových architekturách pro procesory ARM.

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 pravidelně se zúčastňoval konzultací, kde diskutoval stávající stav práce a své následující kroky.

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

Výsledek práce splňuje zadání. Výstupem je aplikace pro operační systém Android, která obsahuje škodlivý kód a umožňuje vzdálenému útočníkovi přístup do zařízení oběti. Zadání z důvodu pochopení principu útoku vyžadovalo podrobnější nastudování vláknového zpracování v jádře operačního systému Linux i instrukční sadu pro danou architekturu cíleného procesoru. Proto se mi jeví zadání jako mimořádně náročné a i tak je text čtivý a bohatý na informace, které jsou důsledně referovány v rámci textu mezi kapitolami. Výslednou aplikaci jsem si vyzkoušel ve virtuálním prostředí a jsem spokojen s výsledky. Budoucí rozšíření práce vidím v zahrnutí architektur pro 32-bitové procesory ARM.

Podpis vedoucího práce: