FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Jana Ernekerová
Vedoucí: práce:	Ing. Tomáš Čejka, Ph.D.
Název práce:	Analysis and detection of KRACK attack against WiFi infrastructure
Obor:	Počítačová bezpečnost

Datum vytvoření: 27. 1. 2019

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 se týká problematiky zranitelnosti bezdrátových sítí Wi-Fi infrastruktury, která byla zveřejněna v posledních letech. Závěrečná práce obsahuje důkladně zpracovanou analýzu a vytvořené prototypy nástrojů pro testování zranitelnosti a detekci podezřelého provozu, který souvisí se zkoumanou zranitelností.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*95 (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:
Text práce je na vysoké úrovni, přehledně členěný a jazykově velmi zdařilý. Rozsah práce splňuje požadavky diplomové práce.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*95 (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:
Práce obsahuje vytvořené zdokumentované skripty, které se dají použít k otestování zranitelných zařízení a zároveň k detekci podezřelého provozu, který s velkou pravděpodobností představuje pokus o zneužití zranitelnosti.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*85 (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:

Výsledkem jsou spustitelné skripty pro detekci pokusů o zneužití zranitelnosti a vytvořené prostředí pro opětovné testování zranitelných zařízení. Vytvořené nástroje včetně konfigurace hardwarových prostředků jsou využitelné pro prezentační a výukové účely a je možné problematiku ukázat na akcích jako je Den otevřených dveří FIT ČVUT v Praze. Bylo by vhodné zobecnit detekční skripty tak, aby byly schopny identifikovat obecné neobvyklé chování zařízení v bezdrátové síti - v tuto chvíli se jedná o jednoúčelovou detekci.

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 se práci věnovala velice intenzivně, dokázala pořídit specifický hardware, který umožňoval pracovat v monitorovacím režimu a odesílat volitelné 802.11 rámce potřebné k simulaci útoku. Mnohé obtíže a překážky se studentce podařilo vyřešit.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*98 (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:

Přestože se práce zabývala již známou zveřejněnou zranitelností, ukázalo se, že zreprodukovat zranitelnost je netriviální a kromě potřeby speciálních chipsetů síťových karet je k úspěšnému útoku nutná řada speciálních okolností. Studentka dokázala v relativně krátkém čase nastudovat rozsáhlou problematiku protokolu 802.11 včetně bezpečnostních rozšíření a princip útoku, který se na specifikaci odkazuje. Práce je napsaná v angličtině, což výrazně podporuje již tak vysokou kvalitu odevzdané práce.

Podpis vedoucího práce: