FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Tomáš Pšenička
Oponent práce:	Ing. Tomáš Čejka, Ph.D.
Název práce:	Analýza útoků KRACK
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 10. 6. 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:
Cílem práce bylo analyzovat zranitelnosti KRACK a vytvořit testovací prostředí. Obojí bylo splněno a popsáno v textu závěrečné práce.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*89 (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 práce je srozumitelný, dobře členěný a čitelný. Umístění některých prvků jako tabulka či diagramy na některých místech není řešeno ideálně a vede čtenáře k listování a hledání vysvětlení v textu (např. Tabulka 2.1, na kterou se odkazuje až v Kapitole 3). U některých citovaných zdrojů není snadno rozpoznatelné, k čemu v textu se citace vztahuje.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*89 (B)*

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:
Výsledkem práce je reálné funkční zapojení, nastavení a zprovoznění testovacího prostředí WiFi sítě. V rámci práce vznikl navíc skript pro dešifrování a dekódování paketu na základě známé nešifrované podoby (plain text). Přiložené CD obsahuje zdrojové kódy hostapd a skripty pro realizaci útoků, ale student dostatečně neoznačil, zda-li tyto zdrojové kódy ve své práci nějak modifikoval, případně kde a jak.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*90 (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:

Tato závěrečná práce srozumitelně vysvětluje princip útoků KRACK proti WiFi infrastruktuře a jejím klientům. Výsledky práce, tj. text práce i nepísemné výstupy, mohou být využity pro výukové účely. Přestože se jedná o již opravenou zranitelnost, stále existují neaktualizovaná zařízení a z toho důvodu je tato práce přínosná a může sloužit k lepšímu pochopení bezpečnostních rizik.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*

5. Otázky k obhajobě

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

Otázky:

V textu je vysvětlen postup dešifrování obsahu komunikace pro jeden paket. Bylo by možné dešifrovat i zbytek komunikace? Co by k tomu bylo případně potřeba?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*90 (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:

Odevzdaná závěrečná práce je pečlivě zpracovaná a analýza zranitelnosti je podrobně popsaná v textu práce. Výsledkem práce je funkční ukázka zneužití zranitelnosti na reálných zařízeních, tuto ukázku je student schopen předvést a vysvětlit. Díky tomu jsou výsledky práce vhodné např. pro studijní/výukové účely. Jako nedostatek práce vnímám nedostatečně označené přínosy studentovy práce v souborech přiložených na CD. Vzhledem k tomu, že student vychází z existující práce, je pro čtenáře poměrně obtížné rozpoznat, které části byly pouze převzaty a které vznikly nově.

Podpis oponenta práce: