FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Jakub Kaloč
Oponent práce:	Ing. Tomáš Čejka, Ph.D.
Název práce:	Bezpečnostní analýza SOHO směrovačů
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 11. 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:
Práce obsahuje rešerši standardů, které se zabývají bezpečností a bezpečnostním testováním. V praktické části práce student provedl analýzu 3 SOHO směrovačů podle nastudované metodiky.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*90 (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:
Rozsah práce je delší než je zvyklostí pro bakalářskou práci. Po jazykové stránce práci nejsem schopen zhodnotit. Text práce se zdá být v pořádku, nedostatky jsou pouze drobné. Vzhledem k počtu stránek bych doporučoval vynechat méně relevantní podrobnosti.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*80 (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:
Nepísemnou částí práce jsou snímky obrazovky a výsledky testů 3 vybraných zařízení. Soudě podle textu práce i přiložených obrázků vypadá testování velice povrchní (nekompletní). Příkladem je skenování pomocí nmap(1), které bylo zřejmě provedeno pouze pomocí protokolu TCP. Pokud autor prováděl další testy, které neobjevily otevřené porty či potenciální zranitelnosti, mělo by to být uvedeno v práci. Je škoda, že student netestoval open source distribuci OpenWrt, která je určená pro bezdrátové směrovače a stala se základem pro TurrisOS (od sdružení CZ.NIC) a nebo přímo směrovač Turris (Omnia), který je vyvíjen a prezentován jako výkonný směrovač zaměřený na bezpečnost.

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:
Pozitivně hodnotím především rešeršní část práce, která mapuje mezinárodní a české standardy a normy, které se týkají bezpečnosti. Zvolená metodologie testování i samotné testování existujících domácích směrovačů působí spíše jako příklad použití než jako komplexní podrobné otestování zabezpečení vybraných směrovačů.

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:
Byly ve veřejně dostupných zdrojích pro testovaná zařízení nalezeny nějaké známé neopravené zranitelnosti?
Byly provedeny testy zranitelností webového rozhraní?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*85 (B)*

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:
Relativně dlouhou část práce tvoří rešerše, která shrnuje nejdůležitější používané standardy a normy. Vysvětlená existující metodologie hodnocení bezpečnostních zranitelností je následně využita v praktické části, kde student testuje 3 vybrané domácí směrovače. V závěru praktické části podle mého názoru chybí celkové shrnutí testů a celkové vyhodnocení vybraných zařízení. Práce vyznívá tak, že pokud uživatel vypne testované služby a nastaví silná hesla, budou zařízení dostatečně zabezpečeny. Zůstává otázkou, zda-li to tak skutečně je, neboť testy se nezdají být dostatečně důkladné.

Podpis oponenta práce: