FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Tomáš Vondra, Ph.D.
Student:	Gabriel Seidl
Název práce:	Bezpečnostní analýza routeru D-Link DIR-842
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	17. února 2023

Hodnotící kritéria

1. Splnění zadání

▸ [1] **zadání splněno**
[2] zadání splněno s menšími výhradami
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Zadání bylo splněno. Nebylo v něm specifikováno, z jakého směru má být bezpečnost routeru prozkoumána. Líbí se mi přístup, kdy student prozkoumal většinu přístupů k analýze zařízení.

2. Písemná část práce 100 / 100 (A)

Práce je rozsahově přiměřená, neobsahuje věcné chyby. Struktura je logicky správně a text se dobře čte. K typografické stránce a použití citací také nemám výhrad.

3. Nepísemná část, přílohy 100 / 100 (A)

Osobně bych k analýze UPnP využil existující software, např. Miranda-UPnP, nicméně vzniklý jednoduchý nástroj v Pythonu a jeho popis v textu může ostatním usnadnit studium tohoto protokolu. Také oceňuji práci s analýzou chybné implementace AES v zařízení. Dekódovací nástroj zřejmě může usnadnit obnovu hesel ze záloh nastavení, pokud by byla potřeba.

4. Hodnocení výsledků, jejich využitelnost 100 / 100 (A)

Nejlépe využitelná mi připadá možnost injekce příkazů, která sice již byla objevena, ale chápu-li správně, nebylo snadné ji na Internetu objevit. Byla nalezena až po analýze souboru s firmwarem zařízení. Cesta k ní sice vyžaduje administrátorský přístup k zařízení, ale toho lze dosáhnout hádáním hesel. Mimo útočníka dovoluje ovládnout

zařízení i uživateli, který pak může lépe využít svůj hardware, např. si zapnout funkci VLAN nebo instalovat VPN.

Celkové hodnocení

100 /100 (A)

Práce je dobře psaná a lze ji použít i jako návod pro analýzu podobných zařízení. Mimo očekávatelné zranitelnosti UPnP byla objevena i injekce příkazů, která umožní kompletní ovládnutí zařízení. Analýza byla provedena snad ze všech možných úhlů mimo WiFi, která byla deklarována jako mimo rámec práce a hledání otevřených sériových nebo debugovacích portů na desce zařízení, které ale nebylo nutné, protože desku lze ovládnout bez něho.

Instrukce

Splnění zadání

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.

Písemná část práce

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. 52/2021, 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.

Nepísemná část, přílohy

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.

Hodnocení výsledků, jejich využitelnost

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.

Celkové hodnocení

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.