FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš
Student:	Gabriel Seidl
Název práce:	Bezpečnostní analýza routeru D-Link DIR-842
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	26. května 2023

Hodnotící kritéria

1. Splnění zadání

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

Všechny body zadání jsou splněny, i když v některých částech spíše u spodní hranice toho, co bylo očekáváno.

2. Písemná část práce 75 / 100 (C)

Písemná část práce je nevyrovnaná. Kapitola 2 je dosti chudá a z větší části nepříliš relevantní; obětoval bych sekce 2.1, 2.2, 2.6 a implementační část 2.5 a naopak se zaměřil na bezpečnostní aspekty sekcí 2.3-2.5. Také kapitola 3 by si zasloužila výrazně detailnější zpracování, mimo jiné považuji za důležité vyznačit i části, které byly zkoumány a autor je neshledal problematickými. Naproti tomu kapitoly 4 a 5 jsou zpracovány pěkně, jdou do potřebné hloubky a vhodně interpretují zjištěné nedostatky. Citelně však chybí aspoň základní analýza možností, jak by útočník mohl zranitelnosti zneužít z vnější sítě, např. prostřednictvím útoků typu Server Side Request Forgery.
Po jazykové stránce je práce spíše v pořádku, až na čárky. Dráždí mě "internet" s malým "i" i na začátku vět, nadpisů nebo v seznamu zkratek, zjevně důsledek search&replace.

3. Nepísemná část, přílohy 90 / 100 (A)

Nepísemná část práce odpovídá zaměření textu. Přiloženy jsou zejména programy, kterými student ověřoval své hypotézy, dále pak důležité komponenty, jichž se analýza týkala - vyextrahovaný firmware, implementace D-Linkového pseudoAESu. Podle mě je to přiměřené.

4. Hodnocení výsledků, jejich využitelnost 70 /100 (C)

Na výsledcích práce se negativně projevilo její odkládání. V době, kdy byla práce zadána, bylo její zaměření relevantní a výsledky by jistě byly přínosné pro uživatele. V době obhajoby je jejich uplatnitelnost podstatně horší. Dovedu si ji ale dobře představit jako výchozí bod pro analýzy novějších routerů D-Link - zejména z ohledu prozkoumání, zda je stále používán špatný šifrovací algoritmus nebo prehistorický obsah firmware.

5. Aktivita studenta

[1] výborná aktivita
[2] velmi dobrá aktivita
[3] průměrná aktivita
▸ **[4] slabší, ale ještě dostatečná aktivita**
[5] nedostatečná aktivita

Aktivita studenta byla spíše sporadická a s dlouhými prodlevami mezi aktivními obdobími.

6. Samostatnost studenta

[1] výborná samostatnost
[2] velmi dobrá samostatnost
▸ **[3] průměrná samostatnost**
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Celkové hodnocení 75 /100 (C)

Výsledkem práce studenta je bezpečnostní analýza routeru, který byl v době řešení ještě stále dodáván zákazníkům a tedy dosažená zjištění by byla užitečná; tento přínos byl však bohužel umenšen prodlevou s obhajobou. Jednoznačně kladně hodnotím, že student analýzu dokončil a že se mu podařilo najít některé zranitelnosti, včetně použití velmi špatného šifrovacího algoritmu, jehož slabost demonstroval jeho prolomením. Méně spokojen jsem s provedením, které sice není vysloveně špatné, ale zůstává daleko za potenciálem studenta i tématu. Je to hodně vidět na textu, jehož některé kapitoly působí, jako kdyby je student napsal jen proto, že je požadovalo zadání a nedalo se jim proto vyhnout. Celkový výsledek hodnotím jako dobrý.

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.

Aktivita studenta

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.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

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.