

Posudek práce

předložené na Přírodovědecké fakultě JU

☒ posudek vedoucího
☒ bakalářské práce

☐ posudek oponenta
☐ diplomové práce

Autor/~~ka~~: **Jiří Kudlata**
Název práce: **Odolnost šifrování standardu WPA3 na platformě Mikrotik RouterOS**
Studijní program a obor: **Aplikovaná informatika**
Rok odevzdání: **13. 5. 2023**
Jméno a tituly vedoucího/opponenta: **Ing. Jan Fesl, Ph.D.**
Pracoviště: **Katedra informatiky**
Kontaktní e-mail: **jfesl@prf.jcu.cz**

Odborná úroveň práce:

☐ vynikající ☐ velmi dobrá ☒ průměrná ☐ podprůměrná ☐ nevyhovující

Věcné chyby:

☐ téměř žádné ☒ vzhledem k rozsahu přiměřený počet ☐ méně podstatné četné ☐ závažné

Výsledky:

☐ originální ☒ původní i převzaté ☐ netriviální kompilace ☐ citované z literatury ☐ opsané

Rozsah práce:

☐ veliký ☒ standardní ☐ dostatečný ☐ nedostatečný

Grafická, jazyková a formální úroveň:

☐ vynikající ☐ velmi dobrá ☐ průměrná ☒ podprůměrná ☐ nevyhovující

Tiskové chyby:

☐ téměř žádné ☒ vzhledem k rozsahu a tématu přiměřený počet ☐ četné

Celková úroveň práce:

☐ vynikající ☐ velmi dobrá ☐ průměrná ☒ podprůměrná ☐ nevyhovující

Slovní vyjádření, komentáře a připomínky vedoucího/opponenta:

Předložená bakalářská práce obsahuje zajímavou problematiku týkající se šifrování bezdrátových počítačových sítí resp. nového šifrovacího protokolu WPA3.

Z hlediska splnění zadání konstatuji následující:

- 1) Bakalant v dostatečné míře popsal a vysvětlil mechanismy a algoritmy zabezpečení, které protokol WPA3 používá. Nutno podotknout, že autor čerpal přímo z oficiální certifikace WPA3 od Wifi Alliance a některé pasáže (např. na stranách 10-13) přejal resp. přeložil téměř doslovně. Autor práce však tyto pasáže ocitoval a tudíž nelze v tomto případě hovořit o plagiatorismu v pravém slova smyslu, nicméně práce by zasloužila v rešeršní části většího osobního zasazení.
- 2) Útoky na WPA3 v kapitole 4 jsou popsány poměrně povrchně a zasloužily by taktéž hlubšího zpracování - autor měl vyvinout větší iniciativu a zmínit i další známé útoky jako např. Muted Peer, PMK Gobbler či Memory Omnivore. Nástroje umožňující útoky na WPA3 jsou popsány taktéž stručně a občas i ne zcela srozumitelně (v případě, pokud čtenář nezná problematiku dopředu) viz např. Dragon drain-and-time.
- 3) Praktické otestování resp. provedení útoků prostřednictvím zmíněných nástrojů bylo provedeno v dostatečné míře na platformách Mikrotik RouterOS 7.1, 7.6 a 7.8.

Z hlediska kvality bakalářské práce po písemné a grafické stránce konstatuji toto:

- 1) Práce obsahuje určité množství pravopisných chyb (např. překlipy, čárky ve větách).
- 2) Tabulky na stranách 21, 23 a 24 jsou označeny jako obrázky a nejsou přizpůsobeny formátu stránky.
- 3) Práce používá nestejný styl řádkování a velikosti fontů – viz str. 11 a 22.
- 4) Kapitola zabývající se nástroji umožňující útoky na WPA3 má poměrně chaotické uspořádání, resp. prolíná se s měřeními, což opět nepřispívá ke srozumitelnosti obsahu práce.
- 5) Část výsledků testování (Dragon drain) je pouze součástí přílohy a její popis v textu zcela chybí.
- 6) Závěr práce, který by sumarizoval dosažené dosažené výstupy, opět zcela chybí a výsledné doporučení je velmi stručné.

Z hlediska implementace skriptů pro automatizované testování musím konstatovat, že jejich výsledná kvalita je hraniční, resp. vytvořené řešení je velmi jednoduché tzn. v podstatě jen implementuje uživatelské rozhraní propojující externí testovací nástroje. Rozhodně tedy bylo možné vytvořit bohatší funkcionalitu řešení (umožňující automatickou konfiguraci a update operačního systému RouterOS) – nicméně toto nebylo v zadání práce explicitně vyžadováno.

Celkově lze konstatovat, že práce byla šita horkou jehlou resp. nebyla po písemné stránce zcela dokončena a utrpěla výrazně i po grafické stránce práce zřejmě kvůli tomu, že si autor nenechal na finalizaci práce dostatečnou časovou rezervu. Implementačně autor vytvořil jednoduché avšak funkční řešení a naměřil relativně velké množství výsledků, nicméně tyto ne zcela zahrnul do textu práce a umístil je pouze do příloh. Z pohledu požadavků, které obsahuje originální zadání práce, autor reálně splnil majoritní část těchto požadavků a tento fakt je mém hodnocení zohledněn.

Případné otázky při obhajobě a náměty do diskuze:

Otázky nemám.

Práci

☒ doporučuji

☐ nedoporučuji

uznat jako diplomovou/bakalářskou.

Navrhuji hodnocení stupněm:

☐ výborně ☐ velmi dobře ☒ dobře ☐ neprospěl/a

Místo, datum a podpis vedoucího/oponenta:

V Českých Budějovicích dne 13. May 2023

.....