Posudek oponenta bakalářské práce

Student: Snášel Daniel
Téma: Nasazení a vylepšení nástroje pro zachytávání RDP útoků (id 22251)
Oponent: Hranický Radek, Ing., UIFS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Práci hodnotím jako náročnější, neboť výsledný produkt je poměrně komplexní aplikace. Student v rámci práce navrhl a implementoval několik vzájemně komunikujících subsystémů. Značný prostor byl věnován také provozu vytvořeného nástroje a podrobné analýze získaných dat.

2. Splnění požadavků zadání **zadání splněno**

Zadání považuji za splněné v plném rozsahu.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

4. Prezentační úroveň předložené práce **88 b. (B)**

Práce je logicky členěna a jednotlivé kapitoly na sebe navazují. Teoretická část obsahuje vhodně zvolené a k tématu relevantní informace. V praktické části by bylo vhodné věnovat samostatnou kapitolu návrhu architektury systému a v další se zaměřit na implementační detaily. V práci je návrh částečně v kap. 4, kde je ale také popis existujícího software. V kap. 5 se pak prolíná návrh s implementací. Oceňuji nicméně množství názorných schémat, která ilustrují fungování systému a jeho součástí. Pochopitelnost pro čtenáře zvyšují také příklady záznamů jednotlivých tabulek databáze.

5. Formální úprava technické zprávy **72 b. (C)**

Typografická stránka práce je na vysoké úrovni. Opticky práce působí velice konzistentním a přívětivým dojmem. Totéž bohužel nemohu říci o jazykové stránce. V práci se vykytují sekvence zbytečně strohých vět s často se opakujícími slovy. Některé anglikanismy, např. "payload" či "pomocí webhooku" by šlo nahradit vhodnějšími ekvivalenty. Datum s jednociferným číslem dne či měsíce píšeme bez nuly na začátku. Za tečkou je pak vhodné udělat mezeru.

6. Práce s literaturou **60 b. (D)**

Z celkem 18 zdrojů jsou bohužel jen 4 skutečně odborné publikace z vědeckých žurnálů a konferencí. Mimo několika referenčních manuálů a studentských závěrečných prací jsou vše vesměs online zdroje. Software umístěný na portálu Github nepovažuji za literární pramen. Takovéto "prameny" jsou přitom uvedeny hned tři. Zdroj č. 8 je zvláštní. Neštastné je také odkazování na Wikipedii, byť jen jako poznámka pod čarou. Zejména, když k danému tématu existují vhodnější zdroje.

7. Realizační výstup **95 b. (A)**

Realizační výstup zahrnuje několik vzájemně spolupracujících subsystémů. Rozsahově čítá přes tisíc řádků v jazyce Python. Zdrojový kód je přehledný a dobře komentovaný. Nástroj je funkční a jeho použitelnost mi student prakticky demonstroval. Pro ověření funkčnosti student také implementoval sadu automatizovaných testů.

8. Využitelnost výsledků

O využitelnosti výsledků nemám pochyby. Vytvořený software byl již nasazen ve společnosti Avast.

9. Otázky k obhajobě

- Jaké existující systémy typu honeypot pro protokol RDP znáte? V čem se od nich vaše řešení odlišuje?

10. Souhrnné hodnocení **83 b. velmi dobře (B)**

Student odvedl vynikající programátorskou práci, kterou dokázal přehledně a názorně zdokumentovat v technické zprávě. Na bakalářskou práci se jedná o poměrně netriviální a rozsáhlé dílo. Výsledek bohužel degraduje výběr a citování použité literatury. Slabší je též jazyková stránka textu. S ohledem na obtížnost zadání však lze připustit jistou míru tolerance. Doporučuji hodnocení B.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 24. června 2020

Hranický Radek, Ing.
oponent