Posudek oponenta bakalářské práce

Student: Kolajová Jana
Téma: Analýza vybraných síťových zranitelností (id 20299)
Oponent: Malinka Kamil, Mgr., Ph.D., UITS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

2. Splnění požadavků zadání **zadání nesplněno**

Ačkoliv práce obsahuje všechna potřebná klíčová slova, nepovažuji zadání za splněné. Většina části teoretické přípravy se věnuje spíše obecným principům bezpečnosti bez bližšího zaměření na síťovou problematiku. Zaměření práce nebylo na obecnou metodiku řízení bezpečnosti, která je navíc podána nedostatečným způsobem, ale na jednu konkrétní oblast. Databázi zranitelností NIST je věnovaná jen jedna strana, která navíc opět spíše popisuje organizační strukturu NIST a vlastní databázi se věnuje minimálně atd. Návrh nástroje se pohybuje na minimální úrovni - v podstatě jen stahovač záznamů z webu. V bodě 4. nepovažuji použití metrik ASNM za dostatečné. Zpracování bodu 5 zcela chybí. Na druhou stranu, jakási základní hodnotitelná implementace u bodu 3 a půlky bodu 4 proběhla.

3. Rozsah technické zprávy **splňuje pouze minimální požadavky**

Rozsah zprávy se blíží tomu užšímu konci, což nemusí být vždy negativum. Bohužel v tomto případě je už tak malý obsah práce snížen částmi, které sice jsou vzdáleně relevantní k tématu, ale jen velmi vzdáleně. Chybí hlubší zanoření do problematiky, alespoň v jedné části - ať už u konkrétních exploitů, přehledů síťových zranitelností nebo ASNM metrik .

4. Prezentační úroveň předložené práce **40 b. (F)**

Logická struktura se na první pohled jeví v pořádku. Při bližším čtení se projevuje špatná orientace autora v celé problematice. Po neexistujícím uvedení do problematiky se pak teoretická část práce věnuje obecnému řízení bezpečnosti v systému, což je vzhledem k úzce definovanému tématu nevhodné. Není pak věnován dostatečný prostor pro ponoření do hloubky. Tento trend je pak i v dalších částech práce, kdy obsahuje některé zbytečné pasáže. Autorka dále přeskakuje mezi různými úrovněmi abstrakce a povyšuje některé technikálie na obecné principy. Práce obsahuje špatně přeložené pasáže, kterou jsou dány do špatného kontextu. Např. na str. 14. se kapitola realizace síťových útoků zabývá pouze oblastí penetračního testování, což já vnímám ne jako útoky, ale preventivní opatření. Opět chybí jakékoliv technické zanoření např. až na úroveň konkrétního útoku, podkapitola v podstatě jen konstatuje, že existují nástroje, a že asi i fungují. Totéž pro část k detekci útoků - opět jen hrubé shrnutí základních principů. Práce navíc obsahuje několik tvrzení, které by vysokoškolská práce se zaměřením na bezpečnost neměla obsahovat. Např. str. 10: "Cílem je prevence. Aby designeři a programátoři nevkládali do svých produktů zranitelnosti."

5. Formální úprava technické zprávy **30 b. (F)**

Formální úprava práce je naprosto nedostatečná! Např. na str. 9 jsem v jednom krátkém odstavci napočítal 7 pravopisných chyb. Evidentně nebylo ani využito automatických nástrojů pro kontrolu, autorka si snad práci po sobě ani nepřečetla. Práce obsahuje mnoho typografických prohřešků - je použitý špatný formát pro odkazy na citace (alespoň, že byl konzistentní přes celou práci), některé obrázky jsou bez popisu, mezery mezi řádky nejsou konzistentní (např. str. 19), špatné pomlčky a mnoho dalšího.

6. Práce s literaturou **50 b. (E)**

Autorka poměrně rozumně odkazuje na externí zdroje, ovšem v některých oblastech neprokázala, že všemu dobře porozuměla. Asi nejzásadnější výtka je pak k vysokému stáří použitých zdrojů. S tím souvisí i některá tvrzení např. viz strana 8: "Třetí generace byla představeno teprve nedávno (12.12.2014), ale zatím není oficiálně použita." Dalším velkým nedostatkem je také absence referencí a kontextu k ASNM metrikám. V celém textu jsem nenašel vysvětlení zkratky, nebo odkaz na metodologii, což, vzhledem k tomu, že je to jeden z explicitních bodů zadání, považuji za fatální. Tomu odpovídá i obsahové zpracování posledního bodu, který v podstatě jen prezentuje spoustu síťových hodnot bez dalšího kontextu.

7. Realizační výstup **50 b. (E)**

Realizační výstup obsahuje tři skripty v jazyce Python, celkem do 300 řádků. Totéž potom v upravené variantě po změně na straně NIST. V podstatě je to stahovač informací z webu, které jsou pak uloženy v jednoduché databázi. Řekněme, že jako celek se to dá považovat za jakousi minimalistickou funkční implementaci bodu 3. zadání. Kód má poměrně dobrou štábní kulturu, je málo okomentovaný. Pozitivně hodnotím, že stahování fungovalo i po drobných změnách na straně NIST.

8. Využitelnost výsledků

Práce vypadá jako shluk zdánlivě relevantních souvisejících výtažků ze zdrojů bez hlubší porozumění autora a větší snahy vše nějakým způsobem integrovat do logicky souvisejícího samonosného celku. Nevidím žádnou možnost využití výsledků práce v praxi.

9. Otázky k obhajobě

-

10. Souhrnné hodnocení **45 b. nevyhovující (F)**

Studentka se dotkla všech částí nutných pro úspěšné dořešení bakalářské práce, ale nikde si nedokázala širokou problematiku zúžit natolik, aby ji dokázala smysluplně zpracovat a prokázala hlubší porozumění. Jedním z příkladů může být podkapitola "Typy útoků", která by v podstatě měla plně naplňovat 1. bod zadání. Na 1 straně ovšem obsahuje jen naprosto základní rozdělení útoků na pasivní a aktivní, což je zcela nedostatečné. Splnění některých bodů zadání je na hraně akceptovatelnosti, některé body jsou nesplněny. Povrchní zpracování tématu bez viditelného prokázání hlubšího vhledu alespoň v jedné z oblastí se pak projevují i na výsledném hodnocení. Práci jako celek považuji za nedostatečnou a nedoporučuji k obhajobě.

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

V Brně dne: 1. června 2017

.....
podpis