Posudek oponenta bakalářské práce

Student: Eisner Michal
Téma: Vliv síťové infrastruktury na distribuované lámání hesel (id 21889)
Oponent: Zobal Lukáš, Ing., UIFS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Pro úspěšné vypracování práce bylo nutné nastudovat problematiku lámání hesel, seznámit se s existujícími nástroji Fitcrack a Hashtopolis a navrhnout vhodné síťové topologie. Zadání je hodnoceno jako průměrně obtížné.

2. Splnění požadavků zadání **zadání splněno**

Všechny body zadání byly splněny.

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

Práce je v obvyklém rozsahu, cca 60 normostran. Obsah je informativní a neobsahuje duplicity. Obrázky 4.1 a 4.2 jsou spíše doplňující hodnoty.

4. Prezentační úroveň předložené práce **70 b. (C)**

Na nejvyšší úrovni kapitol je práce rozdělena logicky a odpovídá zadání. Některé sekce jsou velmi stručné a zvážil bych jejich rozšíření či sloučení tak, aby jich nebylo na jedné straně například 8. Velmi nepřehledné je ovšem značení grafů, kdy se autor uchýlil ke značení (a,b,c,...), kde každé písmeno reprezentuje relativně velké množství informací a informativní hodnota grafů je tak snížena. Zároveň by v grafech bylo vhodné odlišit jednotlivé topologie tak, aby je bylo možné mezi sebou porovnat. Každý graf pak nese zajímavé výsledky, které bohužel nejsou autorem nijak rozebrány ani vysvětleny a je uvedeno jen shrnující hodnocení výsledků experimentů (Například graf 5.1 - po bližším zkoumání zjistíme, že s rostoucím počtem uzlů se rychlost lámání u Fitcracku zvyšuje, zatímco u Hashtopolis se snižuje - nejen že toto chování není vysvětleno, ale tato informace není kvůli formě grafu zřejmá a hodnoty působí spíše náhodně).

5. Formální úprava technické zprávy **75 b. (C)**

Práce obsahuje nemalé množství překlepů. Autor také často mluví v ich-formě a sklouzává v vyprávěcímu stylu, který se do bakalářské práce nehodí. Jinak ale k formální úpravě nemám větší výtky.

6. Práce s literaturou **80 b. (B)**

Některé citace mají překlepy a chybí jim zásadní informace jako rok vydání nebo typ práce. Jinak je však literatura vhodně volena a to ve vhodném rozsahu.

7. Realizační výstup **75 b. (C)**

Implementované skripty v Pythonu jsou tvořeny několika stovkami řádků a jejich rozsah je odpovídající. Jedná se o skripty pro automatizaci experimentů. Struktura členění tohoto projektu však není ideální a kód se zbytečně duplikuje na několika místech. Po bližším zkoumání se v kódu nachází chyby, které se však projevily jen v pomocných výpisech. Celkově by realizačnímu výstupu prospěl lepší návrh, což se ovšem vzhledem k jeho použití (jako pomocné skripty pro automatizaci) dá pochopit.

8. Využitelnost výsledků

Práce vyhodnotila dopady síťové infrastruktury na lámání hesel pomocí nástrojů Fitcrack a Hashtopolis. Díky tomu byly identifikovány hlavní problémy nástroje a výsledky je možné využít k dalšímu vylepšení nástroje Fitcrack.

9. Otázky k obhajobě

1) Jaké je Vaše očekávání dopadu síťové infrastuktury na zbývající typy útoků - kombinační a hybridní - v nástrojích Fitcrack a Hashtopolis?

10. Souhrnné hodnocení **75 b. dobře (C)**

Cílem práce bylo zjistit vliv síťové infrastruktury na distribuované lámání hesel. Student navrhl a provedl experimenty, které tuto informaci poskytly. Práce občas sklouzává k vyprávěcímu stylu a obsahuje množství překlepů, jinak je však členěna logicky a neobsahuje duplicitní informace. Grafy popisující výsledky experimentů mohly být ve srozumitelnější formě, ale po seznámení se s reprezentací jednotlivých sloupců v nich čtenář nalezne požadované informace. Kladně hodnotím využití protokolu SNMP pro získávání dat.

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

V Brně dne: 25. května 2019

Zobal Lukáš, Ing.
oponent