Posudek oponenta bakalářské práce

Student: Marušic Marek
Téma: Automatizace MitM útoku pro dešifrování SSL/TLS (id 18593)
Oponent: Lichtner Ondrej, Ing., UIFS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Práca vyžadovala naštudovanie bezpečnostných protokolov SSL/TLS a aktuálnych útokov na ne. Zároveň mal študent za úlohu zrealizovať sondu automatizujúcu vykonanie transparentných Man-in-the-Middle útokov na SSL/TLS spojenia a to aj po hardware aj software stránke. Keďže problematika bezpečnostných protokolov SSL/TLS a útokov na nich sa v rámci bakalárskeho štúdia preberá iba okrajovo (ak vôbec) považujem toto zadanie za náročnejšie.

2. Splnění požadavků zadání **zadání splněno s podstatným rozšířením**

Študent úspešne splnil všetky body zadania. Nad rámec zadania študent vytvoril článok prezentovaný na konferencii Excel@FIT, rozšíril funkcionalitu nástroja SSLsplit a vytvorená aplikácia poskytuje konzolové ako aj grafické užívateľské rozhranie čo vedie k veľmi jednoduchému použitiu.

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

Práca je vysádzaná LaTeXovou šablónou a má 36 strán. Je teda v obvyklom rozsahu.

4. Prezentační úroveň předložené práce **80 b. (B)**

Práca je, vzhľadom na riešenú problematiku, členená logicky, s menšími výhradami. Kapitola 4 "Návrh automatizácie" mohla byť rozsiahlejšia alebo spojená s nasledujúcou kapitolou "Implementácia" do kapitoly "Návrh a implementácia".

5. Formální úprava technické zprávy **70 b. (C)**

Po typografickej stránke je práca v poriadku až na jeden pretekajúci riadok na strane 13. Z jazykovej stránky obsahuje práca väčšie množstvo preklepov, pravopisných chýb a zle štylizovaných viet. Do budúcna by som doporučil zamyslieť sa nad písaním záverečnej práce v angličtine, kedže priložený článok z Excel@FIT by som hodnotil jazykovo na lepšej úrovni.

6. Práce s literaturou **80 b. (B)**

Študent v práci cituje z relevantných zdrojov. Niektoré zdroje (napr. RFC, Python dokumentácia) uvedené ako poznámka pod čiarou by som ale umiestnil do hlavnej bibliografie práce.

7. Realizační výstup **90 b. (A)**

Vytvorená aplikácia splňuje všetky požiadavky na funkčnosť a je jednoducho použiteľná. Súčasťou je študentom upravený opensource nástroj SSLsplit, použitý v súlade s licenčnými podmienkami. Podľa demonštrovaných experimentálnych výsledkov sa dá hovoriť o transparentnom prevedení Man-in-the-Middle útoku.

Zdrojový kód samotnej aplikácie je organizovaný iba do troch súborov, samotná funkcionalita aplikácie sa nachádza iba v jednom z nich, zvyšné dva implementujú formátovanie logovacích výstupov a grafické užívatelské rozhranie. Toto vidím ako možný problém z pohladu rozšíriteľnosti aplikácie do budúcna.

8. Využitelnost výsledků

Práca stavia nad už dostupnými nástrojmi na vykonanie Man-in-the-Middle útokov na protokoly SSl/TLS a vytvára aplikáciu, ktorá automatizuje ich použitie spolu s konfiguráciou sieťových zariadení sondy. Takto výrazne zjednodušené prevedenie útoku a zachytávanie konverzácii môže byť jednoducho použitý v oblasti forenznej analýzy.

9. Otázky k obhajobě

1. V tabulke na Obr. 3.1 porovnávate niekoľko nástrojov vykonávajúcich Man-in-the-Middle útok. Pri implementácii ste zvolili SSLsplit, ktorý popisujete ako najhorší z nich. Viete túto voľbu zdôvodnit?
2. Ako náročné by bolo rozšíriť aplikáciu o ďalšie nástroje podporujúce iné scenáre Man-in-the-Middle útokov (napr. iné nástroje zo spomínanej tabulky)?

10. Souhrnné hodnocení **85 b. velmi dobře (B)**

Prácu hodnotím na veľmi dobre (B), vzhľadom na kvalitu realizačného výstupu a jeho použiteľnost vo forenznej analýze. Študent sa nad rámec zadania zúčastnil konferencie Excel@FIT a tiež rozšíril funkcionalitu opensource nástroja SSLsplit.

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

V Brně dne: 1. června 2016

.....
podpis