Review of Master's Thesis

Student: Pastuszek Jakub, Bc.
Title: Extraction of Decrypted Data from SSL Connection (id 22185)
Reviewer: Veselý Vladimír, Ing., Ph.D., UIFS FIT VUT

1. Assignment complexity — **average assignment**

Zadání navazuje na probíhající vědecký výzkum a aktivity v rámci skupiny NES@FIT. Student měl za úkol: a) zhodnotit existující softwarové nástroje pro realizaci man-in-the-middle útoku na SSL/TLS; b) vybrat nejnadějnější z nich a rozchodit na něm zrcadlení dešifrovaného provozu na zvolené rozhraní; c) integrovat výsledek do platformy linuxového routeru NETX. Svým rozsahem a nároky na zpracování se jedná o průměrně těžké zadání.

2. Completeness of assignment requirements — **assignment fulfilled**

Student všechny body zadání splnil.

3. Length of technical report — **in usual extent**

Práce je psána v husté LaTeXové šabloně a má 45 stránek (se všemi "pomocnými provozy" dohromady pak 46 stránek). Ve výsledku je tedy v obvyklém rozmezí (i když spíše blíž k její spodní hranici).

4. Presentation level of technical report — **70 p. (C)**

Práce je logicky členěna do kapitol, které odrážejí plnění jednotlivých bodů zadání. Anglický jazyk práce přispěje k potenciálně větší čtenářské obci, avšak místy je až příliš znát (zejména kostrbaté větné obraty zhoršující pochopení textu), že student tento jazyk nemá plně zvládnutý.

5. Formal aspects of technical report — **60 p. (D)**

Práce je psaná v angličtině, avšak s nezanedbatelným množství chyb - porušování anglického slovosledu SVOMPT, chybějící (ne)určité členy či interpunkce. Rozšířený abstrakt v češtině je také protkán více než únosným množstvím gramatických chyb (chybějící interpunkce, tvary jako "a při tom"). Obrázek 3.3 má složitě interpretovatelnou vypovídající hodnotu.

6. Literature usage — **70 p. (C)**

Student v práci cituje z relevantních zdrojů. Nicméně v bibliografii jsou prameny ve špatném formátu (pravděpodobně vlivem špatných oddělovačů mezi jmény autorů), a to konkrétně [7] a [9]. V literatuře převažují nepříliš stravitelná RFC, jejichž pochopení studentem je v práci patrné. Kromě standardních citací obsahuje práce i související odkazy v poznámkách pod čarou.

7. Implementation results — **75 p. (C)**

Realizace má podobu modulu a několika konfiguračních skriptů, které roubují SSLspit na platformu NETX. Musím ocenit pečlivost testování výsledného řešení (a to jak ve virtuálním, tak fyzickém prostředí), kde právě testy ukázaly výkonnostní limity SSLsplit a naznačily budoucí směr vývoje.

8. Utilizability of results

Tato práce přinesla SSLsplit do NETX routeru a vytvořila tak podmínky pro potenciální podmínky pro využití NETX v prostředí zákonných odposlechů, ale třeba i jako vývojářskou proxy pro ladění aplikačních protokolů.

9. Questions for defence

- Diskutujte možnosti injektáže vlastních dat (např. JavaScriptu) do provozu procházejícího NETX s aktivovaným SSLsplitem.

10. Total assessment — **70 p. good (C)**

Výslednou práci hodnotím jako dobrou (tedy stupněm C). Na jednu stranu student zadání splnil a kvalitně výstup otestoval, na druhou stranu lepšímu hodnocení brání jazyková stránka technické zprávy.

In Brno 6. June 2019

Veselý Vladimír, Ing., Ph.D.
reviewer