Review of Bachelor's Thesis

Student: Vondráček Martin
Title: Automation of MitM Attack on WiFi Networks (id 18596)
Reviewer: Lichtner Ondrej, Ing., UIFS FIT VUT

1. Assignment complexity — **more demanding assignment**

Práca vyžadovala naštudovanie rôznych technológií zabezpečenia bezdôtových sietí, ich zraniteľností a aktuálnych útokov. Úspešné prevedenie Man-in-the-Middle útoku na bezdrôtove siete vyžaduje niekoľko koordinovaných útokov na protokoly, ktoré vytvárajú topológiu bezdrôtovej siete (ARP, DNS, DHCP). Vzhľadom na rozsiahlosť zadania a problematiku útokov na bezpečnosť sietí, ktorá sa na bakalárskom štúdiu preberá iba okrajovo, považujem zadanie za náročnejšie.

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

Študent úspešne splnil všetky body zadania bez výhrad.

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

Práca je vysádzaná LaTeXovou šablónou a má 30 strán. Je teda v obvyklom rozsahu.

4. Presentation level of technical report — **95 p. (A)**

Práca je, vzhľadom na riešenú problematiku, členená logicky na kapitoly, ktoré zrozumiteľne popisujú všetko dôležité a naväzujú na seba. Každá kapitola nakoniec zhrnie najdôležitejšie informácie, ktoré sú potom použité pri návrhu a implementácii riešenia. Kapitola 5 "Man-in-the-Middle attack" by mohla byť rozsiahlejšia.

5. Formal aspects of technical report — **95 p. (A)**

Práca je písaná v angličtine. Po typografickej stránke je bez výhrad. Z jazykovej stránky sa autor občas dopúšťa typických chýb ako chýbajúce/nesprávne členy, nesprávna štylizácia viet, preklepy a podobne. Frekvencia chýb je ale dostatočne nízka a text je plynulo čitateľný.

6. Literature usage — **95 p. (A)**

Študent v práci cituje z množstva relevantných zdrojov, zoznam literatúry obsahuje 32 položiek. V texte sú riadne odkazované.

7. Implementation results — **95 p. (A)**

Vytvorená aplikácia spĺňuje všetky požiadavky na funkčnosť a je jednoducho použiteľná. Je schopná útokov na populárne možnosti zabezpečenia bezdrôtových sietí, čo je v práci podložené množstvom experimentov. Ako ale sám autor uvádza, experimenty sú jednoduchého charakteru, z dôvodu nedostupnosti vybavenia pre väčšie bezdrôtové siete.

Väčšina implementovaného kódu autor organizuje do knižnice, ktorá abstrahuje použitie nástrojov vykonávajúcich jednotlivé kroky Man-in-the-Middle útokov. Nad touto knižnicou je postavená jednoduchá aplikácia, ktorá Man-in-the-Middle útoky automatizuje a je jednoducho použiteľná.

Kód dodržuje ustanovené Python konvencie, je riadne komentovaný a celkovo na vysokej úrovni. Je logicky organizovaný do modulov a mal by byť jednoducho rozšíriteľný.

8. Utilizability of results

Práca stavia nad už dostupnými nástrojmi na vykonanie Man-in-the-Middle útokov cielených na bezdrôtové siete. Vytvorená aplikácia celý proces automatizuje a je tým pádom jednoducho začleniteľná do iných projektov zaoberajúcich sa forenznou analýzou alebo penetračným testovaním. Vlastné uplatnenie v penetračnom testovaní by mohla nájsť aj vytvorená knižnica.

9. Questions for defence

1. Skúšali ste zmerať aký dopad na výkonnosť má úspešný Man-in-the-Middle útok na bezdrôtové siete? Zaujímal by ma dopad na prenosové rýchlosti, dobu odozvy, prípadne zohladniť aj počet pripojených klientov.

10. Total assessment — **95 p. excellent (A)**

Práca bola vypracovaná počas Erasmu na Univerzite v Malte. Textová aj implementačná časť práce je na veľmi vysokej úrovni a má vysoký potenciál využitia, či už vo forenznej analýze alebo pri penetračnom testovaní. Keďže sa jednalo o náročnejšie zadanie, navrhujem hodnotenie A.

In Brno 9. June 2016

.....
signature