Posudek oponenta diplomové práce

Student: Hujňák Ondřej, Bc.
Téma: Systém pro rozpoznávání APT útoků (id 18999)
Oponent: Kačic Matej, Ing., UITS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

2. Splnění požadavků zadání **zadání splněno**
Zadání splněno v plném rozsahu.

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

4. Prezentační úroveň předložené práce **85 b. (B)**
Struktura textu je vyhovující, kapitoly na sebe logicky navazují. Některé části textu jsou méně srozumitelné, ale je to akceptovatelné. Na konci práce mi chybí srovnání detekčních metod nad různými testovacími daty.

5. Formální úprava technické zprávy **90 b. (A)**
K formální úpravě zprávy nemám výhrady, až na nezvyklé řazení referencí. Jazyková úroveň textu je dobrá. Typografie je na dobré úrovni.

6. Práce s literaturou **80 b. (B)**
Práce s literaturou na dobré úrovni. Student mohl lépe zapracovat analýzu současného stavu (state of the art).

7. Realizační výstup **80 b. (B)**
Student využil nástroje RapidMiner pro implementaci detektoru. Pro úspěšné zpracování dat analytickým nástrojem bylo nutné surová síťová data transformovat na toky a poté upravit. Student si všechny pomocné skripty a konfigurace implementoval sám. Implementované řešení je plně funkční.

8. Využitelnost výsledků
Výsledky práce bude možné využít při dalším zkoumání detekce anomálií v síti. Doporučuji práci rozšířit o další detektory a výsledky následně publikovat.

9. Otázky k obhajobě
- Proč navržený detektor detekuje síťové anomálie, když cílem práce bylo detekovat útoky?

10. Souhrnné hodnocení **85 b. velmi dobře (B)**
Vzhledem k tomu, že realizační výstup je dle mého na kvalitní úrovni, hodnotím práci **stupněm B.**

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

V Brně dne: 7. června 2016

.....
podpis