# Posudek oponenta diplomové práce

**Student:** Kadletz Lukáš, Bc.
**Téma:** Anotace NetFlow dat z pohledu bezpečnosti (id 18858)
**Oponent:** Grégr Matěj, Ing., UIFS FIT VUT

**1. Náročnost zadání** — **průměrně obtížné zadání**

**2. Splnění požadavků zadání** — **zadání splněno**

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

**4. Prezentační úroveň předložené práce** — **90 b. (A)**
K prezentační úrovni technické zprávy nemám námitky. Práce je vhodně členěná, kapitoly na sebe navazují a rozsah jednotlivých kapitol považuji za adekvátní.

**5. Formální úprava technické zprávy** — **80 b. (B)**
Technická zpráva je po typografické stránce kvalitně zpracována. Po jazykové stránce také, ale lze nalézt několik chyb a překlepů, které by v práci být nemusely.

**6. Práce s literaturou** — **90 b. (A)**
Práci s literaturou považuji za standardní, jsou využívány relevantní zdroje a citace jsou v souladu s citačními zvyklostmi. Často je odkazována konkrétní stránka práce, což usnadňuje dohledání informací.

**7. Realizační výstup** — **78 b. (C)**
Výstupem práce je aplikace napsaná v programovacím jazyku PHP za využití frameworku Nette. Interně využívá program nfdump pro procházení flow záznamy. Aplikace je použitelná, zdrojové kódy jsou komentované. Některé programové konstrukce mohou ale v budoucnu přinést problémy - např. kontrola IP adresy pomocí regulárního výrazu určeného pouze pro protokol IPv4 (viz Nfdump.php). Také bych od realizačního výstupu očekával, že bude demonstrován nad větším množstvím anotovaných dat. V práci byl projekt testován nad anotací asi 50 událostí, což vzhledem k množství dat, které byly pro řešení práce k dispozici, je zanedbatelný počet.

**8. Využitelnost výsledků**
Systém může využít správce pro jednodušší přehled detekovaných bezpečnostních událostí. Výsledky práce lze tedy dále využít. Práce také představuje vcelku použitelné webové rozhraní pro práci s flow záznamy a záznamy systému Warden a Nemea.

**9. Otázky k obhajobě**
- Jak dlouho přibližně trvá anotace bezpečnostního incidentu, který byl detekován systémem warden? (Od ověření, zda je reportována událost ve flow datech po zobrazení jednotlivých flow záznamů ve web. rozhraní)

**10. Souhrnné hodnocení** — **80 b. velmi dobře (B)**
Práce představuje webový systém, který je schopen zobrazit bezpečnostní události, které byly zachyceny systémem Warden a použít je při anotaci a práci se záznamy NetFlow. Pro anotaci lze také použít detektory projektu Nemea určeného pro nalezení útoků či anomálií. Samotná práce představuje zajímavý první krok, jak by se anotace flow záznamů dala řešit. Pro reálně funkční řešení bude ale potřeba ještě dalšího vývoje - zejména z pohledu zpracování většího množství dat. Práci celkově hodnotím jako velmi dobrou (B).

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

V Brně dne: 30. května 2016

.....
podpis