Posudek oponenta bakalářské práce

Student: Hurta Marek, Bc.
Téma: Detekce útoku uhádnutí hesla v síťovém provozu (id 16958)
Oponent: Grégr Matěj, Ing., UIFS FIT VUT

1. **Náročnost zadání** **obtížnější zadání**
   Zadání považuji za obtížnější, jelikož student musel nastudovat problematiku zpracování velkého množství dat a metody, jak v těchto datech nalézt relevantní informace.
2. **Splnění požadavků zadání** **zadání splněno**
3. **Rozsah technické zprávy** **je v obvyklém rozmezí**
4. **Prezentační úroveň předložené práce** **80 b. (B)**
   Práce má vhodnou logickou strukturu a jednotlivé kapitoly na sebe navazují. Pro lepší pochopitelnost práce pro čtenáře by nicméně bylo vhodné lépe popsat jednotlivé grafy v kapitole 5, jelikož není přímo zřejmé z jakých dat a za jak dlouhý časový úsek byly grafy vytvořeny.
   V části 6.3 je odkazováno na obrázek 6.3, který se nicméně v textu nenachází.
5. **Formální úprava technické zprávy** **90 b. (A)**
   K typografické ani jazykové stránce práce nemám připomínek.
6. **Práce s literaturou** **90 b. (A)**
   Práce cituje relevantní zdroje, k jejich výběru nemám připomínek. Literatura je citována v souladu s citačními zvyklostmi.
7. **Realizační výstup** **90 b. (A)**
   K realizačnímu výstupu nemám připomínek. Zdrojový kód je dostatečně komentován, program byl v práci řádně otestován na velkém množství dat.
8. **Využitelnost výsledků**
   V práci byl implementován modul, který lze dále použít pro framework Nemea. Z pohledu využitelnosti výsledků je tedy práce přínosná a dále použitelná.
9. **Otázky k obhajobě**
   -
10. **Souhrnné hodnocení** **80 b. velmi dobře (B)**
    Práce se zabývá detekcí útoků z dat NetFlow. Pro detekci byla využita histogramová analýza, pomocí které byl porovnáván aktuální síťový provoz se signaturami jednotlivých útoků. V práci postrádám především vyhodnocení dosažených výsledků, kde z práce není jasné, jak je daná metoda úspěšná - kolik útoků bylo detekováno správně a kolik jako false negative nebo false positive. Práce je nicméně napsána srozumitelně a výsledky lze dále použít. Hodnotím tedy práci jako velmi dobrou (B).

V Brně dne: 5. června 2015

.....
podpis