Posudek oponenta bakalářské práce

Student: Kučera Rostislav
Téma: Charakterizace síťového provozu počítačů a jejich skupin (id 25125)
Oponent: Homoliak Ivan, Ing., Ph.D., UITS FIT VUT

1. **Náročnost zadání** **obtížnější zadání**
   Úlohou bolo analyzovať surovú sieťovú prevádzku v počítačoch a ich skupinách a implementovať systém pre detekciu bezpečnostných a prevádzkových anomálií. Zadanie bolo skôr náročnejšie.
2. **Splnění požadavků zadání** **zadání splněno**
   Zadanie bolo splnené vo všetkých bodoch. Nad rámec zadania študent implementoval unikátny Gaussovský model v jazyku C.
3. **Rozsah technické zprávy** **je v obvyklém rozmezí**
   Práce obsahuje 44 vysázených stran a samotný text bez obrázků představuje 37 normostran. Po započítání obrázků se tak práce blíží obvyklému rozsahu.
4. **Prezentační úroveň předložené práce** **80 b. (B)**
   Prezentačná úroveň práce je dobrá, kapitoly sú pre čitateľov zrozumiteľné a logicky na seba nadväzujú.
5. **Formální úprava technické zprávy** **80 b. (B)**
   Po formálnej a typografickej stránke má práca nadpriemernú úroveň, čomu prispela aj vhodná voľba vysádzacieho systému.
   Jazykovú stránku práce som nehodnotil.
6. **Práce s literaturou** **90 b. (A)**
   Práca obsahuje 24 zdrojov, z ktorých veľké množstvo je dostupných online. Študent čerpal z odborných konferenčných a časopisových článkov. Výber literatúry považujem za vhodný a zodpovedajúci. Výčitku mám k citáciám z Wikipédie, ktorá nie je primárnym zdrojom - študent ju však používa predovšetkým na definíciu pojmov.
7. **Realizační výstup** **90 b. (A)**
   Okrem samotného systému na detekciu anomálií v sieťovej prevádzke bol v rámci práce vytvorený pomerne unikátny a plne použiteľný Gaussovský model v jazyku C, ktorý bol navyše plne integrovaný v multi-vláknovom open-source IDS systéme Suricata.
8. **Využitelnost výsledků**
   Práca je založená na teoretických princípoch, ale sama má predovšetkým aplikačný charakter. Výsledky práce sú použiteľné v rámci príspevku na konferenciu.
9. **Otázky k obhajobě**
   - Je Vami vytvorený systém schopný blokovať DDoS útok? Ak áno, ako rýchlo dokáže zakročiť?
10. **Souhrnné hodnocení** **90 b. výborně (A)**
    Celkovo hodnotím prácu stupňom **A - výborne**. Študent vytvoril unikátny systém na vyhodnocovanie anomálií sieťovej prevádzky. Hodnotenie reflektuje kvalitne spracovanú technickú správu aj kvalitný realizačný výstup.

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

V Brně dne: 3. června 2022

Homoliak Ivan, Ing., Ph.D.
oponent