Posudek oponenta diplomové práce

Student: Hurta Marek, Bc.
Téma: Odvozování pravidel pro mitigaci DDoS (id 19930)
Oponent: Krobot Pavel, Ing., UPSY FIT VUT

1. **Náročnost zadání** **obtížnější zadání**
   Zadání práce bylo náročné. Obsahovalo nastudování stávajících metod a systémů pro monitorování a analýzu dat. Hlavní náplní pak bylo vytvoření programu pro automatické generování pravidel pro zmírnění dopadu síťových útoků, včetně důkladného testování.
2. **Splnění požadavků zadání** **zadání splněno**
   Všechny body zadání byly splněny. Z práce je vidět snaha studenta o vytvoření funkčního celku, použitelného pro praktické nasazení.
3. **Rozsah technické zprávy** **je v obvyklém rozmezí**
4. **Prezentační úroveň předložené práce** **89 b. (B)**
   Práce je dobře strukturovaná. Text práce se dobře čte a celá problematika je z něj dobře pochopitelná. Technický text je vhodně doplňován obrázky.
5. **Formální úprava technické zprávy** **85 b. (B)**
   Práce je psána ve slovenském jazyce, a proto nemohu plně posoudit jazykovou stránku práce. Nicméně text práce se dobře čte, nenarazil jsem při jeho čtení na žádné výrazné nedostatky, místy se objevovaly překlepy. V kapitole 7 by měla být záhlaví tabulek spíše v jazyce práce.
6. **Práce s literaturou** **90 b. (A)**
   Student čerpal z velkého množství zdrojů. Nechybí odborné články z konferencí, zabývající se danou problematikou. Práce s citacemi v textu je velmi dobrá
7. **Realizační výstup** **90 b. (A)**
   Výsledkem práce je funkční program, určený pro automatické vytvoření pravidel, určených pro odstranění nežádoucího provozu na síti. Součástí vytvářených pravidel je také jejich ohodnocení, sloužící jako vodítko pro uživatle, usnadňující jejich využití.
8. **Využitelnost výsledků**
   Výsledný program je připravený pro testování a následné nasazení v reálném provozu. Testy nad vybranou datovou sadou a jejich vyhodnocení přináší nové poznatky v oblasti monitorování sítí a obrany proti (D)DoS útokům.
9. **Otázky k obhajobě**
   -
10. **Souhrnné hodnocení** **90 b. výborně (A)**
    Práce se zabývá automatickým vytvářením pravidel pro mitigaci nežádoucího provozu na síti. Výsledkem práce je aplikace, jež by se měla stát součástí stávajícího řešení, používaného v současnosti pro monitorování provozu a detekci nežádoucích událostí. Tato aplikace byla důkladně testována. Z uvedených výsledků je dobře vidět vhodnost použití implementované aplikace spolu s případy, kdy je její nasazení nevhodné. Celkově práce působí odborně, přehledně a má velký potenciál pro využití v praxi.

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

V Brně dne: 5. června 2017

.....
podpis