Posudek oponenta bakalářské práce

Student: Mjasojedov Igor
Téma: Systém pro ochranu před DoS útoky s využitím IDS (id 23110)
Oponent: Fukač Tomáš, Ing., UPSY FIT VUT

1. Náročnost zadání **obtížnější zadání**

Zadání práce si vyžadovalo studium aplikace DDoS Protector, která je stále ve fázi vývoje, dále bylo nutné se seznámit s knihovnou DPDK a detailně prostudovat zdrojové kódy systému Suricata.

2. Splnění požadavků zadání **zadání splněno**

Všechny body zadání byly splněny.

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

Rozsah předložené technické zprávy je v obvyklém rozmezí, obsahuje přibližně 67 normostran textu, který je doplněn relevantními obrázky.

4. Prezentační úroveň předložené práce **100 b. (A)**

Logická struktura práce je na velmi dobré úrovni, jednotlivé kapitoly na sebe logicky navazují, jejich rozsah odpovídá popisované problematice. Text je informačně velmi bohatý a díky názorným obrázkům pochopitelný i pro čtenáře, který se v problematice příliš neorientuje. V závěru práce je také uvedena obsáhlá úvaha o možnosti dalšího vylepšování systému.

5. Formální úprava technické zprávy **95 b. (A)**

Práce je psaná ve slovenském jazyce, proto nejsem schopen posoudit jazykovou stránku práce. Z typografického hlediska práce obsahuje jen minimum chyb (např. chybějící mezery mezi hodnotou a jednotkou).

6. Práce s literaturou **90 b. (A)**

Práce s literaturou je dle citačních zvyklostí a prameny jsou voleny vhodně s ohledem na téma práce. Všechny převzaté prvky jsou odlišeny od autorových, avšak citace použitých obrázku by mohla být uvedena explicitně.

7. Realizační výstup **85 b. (B)**

Realizační výstup je plně funkční, zdrojový kód vytvořený studentem je dostatečně odlišen od převzatého kódu (oddělen ve zvláštním souboru). Kód však není příliš komentován.

8. Využitelnost výsledků

V rámci práce byl systém Suricata rozšířen o podporu DPDK a to hned ve třech režimech, které umožňují napojení na nejrůznější aplikace. Přidání této podpory dále snižuje nároky spojené s režií kopírování paketů a tím urychluje jejich zpracovávání. Systém Suricata byl následně napojen na aplikaci DDoS Protector, což nově umožňuje detekovat nejrůznější síťové útoky a hrozby. Řešení bude dále vyvíjeno a používáno sdružením CESNET.

9. Otázky k obhajobě

Přidáním podpory DPDK do systému Suricata byla odstraněna většina kopírování paketů, paket se však stále kopíruje ze struktury Mbuf do vnitřní reprezentace systému Suricata. Bylo by možné odstranit i toto kopírování a vnitřně pracovat se strukturou Mbuf? Jak náročná by byla realizace takové úpravy a jaký by byl přibližně výkonový přínos?

10. Souhrnné hodnocení **90 b. výborně (A)**

Vzhledem k velmi dobré úrovni technické zprávy a plně funkčnímu řešení uděluji hodnocení **A - výborně**.

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

V Brně dne: 24. června 2020

Fukač Tomáš, Ing.
oponent