Review of Bachelor's Thesis

Student: Carasec Elena
Title: Optimization of DDoS Mitigation Rule Inference (id 24640)
Reviewer: Grégr Matěj, Ing., Ph.D., DIFS FIT BUT

1. Assignment complexity — **more demanding assignment**

Zadání považuji za obtížnější, jelikož správně optimalizovat a rozšířit již hotové metody je složitější, než je navrhnout znovu. Cíl práce je také ověření v reálném prostředí, což je také typicky složitější úloha.

2. Completeness of assignment requirements — **assignment fulfilled**

3. Length of technical report — **in usual extent**

4. Presentation level of technical report — **80 p. (B)**

Práce je logicky členěná a jednotlivé kapitoly na sebe navazují. Očekával bych nicméně podrobnější popis/příklady, které hodnoty z paketů byly vybrány v rámci rozhodovacích algoritmů a proč. V rámci vygenerovaných BPF filtrů lze vidět, že jsou filtry často kombinací hodnoty TTL a velikosti paketu, což považuji pro filtraci reálného provozu za problematické.

5. Formal aspects of technical report — **90 p. (A)**

Práce je psaná v kvalitní angličtině bez nějakých větších prohřešků. Typografická stránka práce je také kvalitní a nemám k ní příliš výhrad. Jednotlivé grafy by sice mohly být podle mě větší, ale na přehlednost to nemá vliv.

6. Literature usage — **95 p. (A)**

V práci je citováno 62 zdrojů, což považuji za nadprůměrné a přesahující standardní práci. V práci je citováno dle zvyklostí a v souladu s normami. Zvolené citace jsou vcelku dobře vybrány a referovány, takže k práci s literaturou nemám výhrady.

7. Implementation results — **70 p. (C)**

Programové řešení obsahuje několik skriptů v jazyce python, které analyzují pcap soubory a generují BPF filtry. Práce využívá již některé skripty vytvořené již v rámci předchozí BP. Kód je spustitelný, vcelku jednoduchý a čitelný.

V práci mi chybí ale jakékoliv porovnání/změření doby běhu algoritmu, náročnost na výpočetní prostředky a diskuze/komentář nad efektivností vygenerovaných pravidel.

8. Utilizability of results

Práce rozšiřuje stávající práci a optimalizuje algoritmy použité pro detekci útoku. Může sloužit pro další a podrobnější testování těchto algoritmů v reálném provozu.

9. Questions for defence

- Jak velké jsou standardně LEGIT/ATTACK pcap soubory dodané DDoS protectorem pro zpracování v rámci vaší metody? Jak dlouho trvá analýza těchto dat vaším algoritmem?
- Dokázal by daný algoritmus fungovat také z NetFlow/sFlow dat nebo je nutné vždy využít pcap?

10. Total assessment — **85 p. very good (B)**

Práce si klade za cíl optimalizovat algoritmy, které generují pravidla pro eliminaci a filtraci DDoS útoků. Teoretická stránka práce je kvalitní, jak množstvím sestudované literatury, prezentační i typografickou stránkou. V práci bych očekával diskuzi k náročnosti a době běhu daného algoritmu a zhodnocení vytvořených pravidel. Celkově hodnotím práci jako velmi dobrou (B).

In Brno 3 June 2022

Grégr Matěj, Ing., Ph.D.
reviewer