Posudek oponenta bakalářské práce

Student: Škápik Anton
Téma: Detekce volumetrických útoků DoS a DDoS v reálném čase na L3 síťové vrstvě (id 21172)
Oponent: Grégr Matěj, Ing., Ph.D., UIFS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Nutnost seznámit se s novým rozšířením protokolu BGP, ke kterému je často obtížné najít relevantní dokumentaci a propojit ho se systémem detekce útoků, považuji za netriviální záležitost. Zadání tedy hodnotím jako obtížnější.

2. Splnění požadavků zadání **zadání splněno**

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

4. Prezentační úroveň předložené práce **75 b. (C)**

Práce je pochopitelná. Některé části by mohly být popsány podrobněji - např. kapitola testování, kde by bylo vhodné okomentovat jednotlivé příkazy použité pro generování provozu.

5. Formální úprava technické zprávy **85 b. (B)**

Práce je psaná slovensky, s mými znalostmi slovenštiny mi práce přišla čitelná jen s pár překlepy. Typograficky je práce standardní, pouze příklady v části 6.1.2 by mohly být prezentována vhodněji.

6. Práce s literaturou **70 b. (C)**

Práce cituje relevantní standardy. Výhrady mám k citaci [14], která je ve formátu, kdy nelze dohledat zdroj. Formát citací by také mohl být jednotný - např. [13] cituje RFC, bez url, i když ostatní RFC jsou citovány s URL, nebo [8], kde se nepoužívá stejného zkracování jména jako u jiných citací.

7. Realizační výstup **70 b. (C)**

V práci jsou prezentovány dva hlavní body realizačního výstupu: Perl skripty pro generování konfigurace pro BGP směrovač a C++ kód pro zpracování streamu NetFlow dat. Z práce není příliš jasné, co vše implementoval student sám, jelikož např. generování BGP konfigurace bylo v nástroji DDoS defender implementované již před několika lety (copyright ve skriptech je 2014). Není tedy jednoznačně patrné, co je vlastní přínos. Část výsledku je C++ kód, rozumně strukturovaný. Postrádám zdůvodnění, proč je kód psán v nejnovějším C++ standardu, který není na CentOS7 standardně dostupný. Vhodné by bylo také otestovat plugin v rámci reálného prostředí pro zjištění množství false positive.

8. Využitelnost výsledků

Práci byla použita pro rozšíření systému DDoS defender od firmy Flowmon a.s. Jedná se tedy o praktické využití výsledků.

9. Otázky k obhajobě

- Vzhledem k tomu, že kód perl skriptů je totožný se skripty ve standardním instalačním balíčku flowmon, jaký je váš vlastní přínos?
- Nedojde ke zvýšenému zatížení exportéru, při snížení aktivního timeoutu na 1s?

10. Souhrnné hodnocení **70 b. dobře (C)**

Práce si klade za cíl urychlit detekci DDoS útoku na základě NetFlow dat a provést mitigaci pomocí BGP Flowspec. Text práce je psán srozumitelně a realizační výstup lze využít v praxi. V práci mi chybí zdůraznění vlastního přínosu a podrobnější otestování detekce útoků. Práci celkově hodnotím jako dobrou (C).

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

V Brně dne: 31. května 2018

.....
podpis