Posudek oponenta bakalářské práce

Student: Litwora Martin
Téma: Potlačení DDoS útoků s využitím IDS/IPS (id 23121)
Oponent: Tisovčík Peter, Ing., UPSY FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Práce vyžadovala naštudovanie informácií o DDos útokoch, spôsobe ich potlačenia a analyzovanie možnosti využitia existujúcich IDS/IPS systémov k potlačeniu DDos útokov so zameraním na systém Suricata.
Ďalej bolo potrebné vytvoriť návrh a implementovať systém pre potlačenia DDoS útokov.

2. Splnění požadavků zadání **zadání splněno**

Študent vytvoril niekoľko pravidiel na detekciu rôznych typov DDoS útokov. Tieto pravidlá boli následne nasadené do systému a bola otestovaná ich úspešnosť. Pre automatizáciu testovacieho prostredia boli vytvorené potrebné skripty. Zadanie bolo splnene vo všetkých bodoch.

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

Práca obsahuje popis všetkých požadovaných častí v odpovedajúcom rozsahu.

4. Prezentační úroveň předložené práce **85 b. (B)**

Text technickej správy je vhodne štrukturovaný. Najskôr boli uvedené rôzne typy DDoS útokov a IDS/IPS systémov. Následne bol popísaný systém Suricata, za ktorým nasledoval návrh systému pre potlačenie DDoS útokov. V návrhu boli vytvorené potrebné pravidlá, následne bolo implementované testovacie prostredie a koniec správy uzatvárajú výsledky testovania.

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

Text práce obsahuje niekoľko nedostatkov, typografické chyby a preklepy.

6. Práce s literaturou **80 b. (B)**

Práce obsahuje 51 referencí, na ktoré sa v texte korektne odkazuje. Všetky referencie súvisia s tématom práce, vytkol by som ale samotné zdroje, ktoré by mohli byť relevantnejšie. Niektoré referencie, ktoré sa odkazujú na stránky, mohli byť nahradené kvalitnými vedeckými publikáciami.

7. Realizační výstup **85 b. (B)**

Autor vytvoril sadu skriptov a konfiguračných súborov pre prípravu testovacieho prostredia. Zdrojové kódy tiež obsahujú vytvorené pravidlá popísané v práci.

8. Využitelnost výsledků

Výsledky tejto práce sú ďalej využiteľné v praxi v rámci aktivít združenia CESNET pri vývoji akcelerovaného zariadenia pre ochranu pred DDoS útokmi.

9. Otázky k obhajobě

- Aký typ útokov bol pravidlami najlepšie a najhoršie detekovateľný a s akou úspešnosťou?

10. Souhrnné hodnocení **80 b. velmi dobře (B)**

Táto práca obsahuje rozsiahly popis DDoS útokov a spôsobov, akými boli vytvorené pravidlá pre detekciu týchto útokov. Následne bol vytvorený testovací systém, pomocou ktorého sa vyhodnotili výsledky dosiahnuté pri detekcií útokov za pomoci vytvorených pravidiel. Navrhujem preto hodnotenie **B (veľmi dobre)**.

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

V Brně dne: 3. června 2021

Tisovčík Peter, Ing.
oponent