Posudek oponenta bakalářské práce

Student: Pastuszek Jakub
Téma: Detekce síťových útoků analýzou informací z hlavičky HTTP (id 18779)
Oponent: Grégr Matěj, Ing., UIFS FIT VUT

1. Náročnost zadání — **průměrně obtížné zadání**

2. Splnění požadavků zadání — **zadání splněno**

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

4. Prezentační úroveň předložené práce — **70 b. (C)**
Technická zpráva je rozumně členěna, někdy ale chybí podrobnější vysvětlení. Výtky mám zejména k části 8.1.2.4, kde je popis testování nad reálným provozem. Závěry z této části nepovažuji za správné - zejména výpočet míry nesprávně detekovaných útoků.

5. Formální úprava technické zprávy — **68 b. (D)**
Práce je obecně čitelná, nicméně lze najít překlepy a chyby ve shodě podmětu s přísudkem. U některých vět také chybí sloveso, což dělá text v některých pasážích hůře čitelným. Co se týče typografické stránce práce tak by bylo asi vhodnější ji napsat v něčem jiném než ve Wordu, ale jinak k ní nemám výhrady.

6. Práce s literaturou — **70 b. (C)**
Práce s literaturou je standardní. Výtku mám nicméně k citaci [12], která je v seznamu literatury, nicméně na ní není nikde v textu odkazováno.

7. Realizační výstup — **70 b. (C)**
Výstupem práce jsou skripty, které umožňují zpracovat anotovaná data NetFlow a reportovat, zdali došlo k útoku. Pravidla použitá pro detekci útoku ale nelze načíst z externího souboru a je nutné upravit přímo daný skript. Regulární výrazy, které jsou použity ve skriptu také nepovažuji za kompletní přepis všech pravidel z přílohy A.

8. Využitelnost výsledků
Skripty lze do jisté míry použít pro detekci útoků nad zachycenými daty NetFlow. Díky tomu, že nelze jednoduše upravovat vyhledávané výrazy, případně si vytvořit výrazy vlastní, nepovažuji práci do budoucna za příliš použitelnou.

9. Otázky k obhajobě
-

10. Souhrnné hodnocení — **70 b. dobře (C)**
Práce si klade za cíl zjistit zda-li lze flow záznamy rozšířené o informace protokolu HTTP k detekci útoků. Pro samotnou detekci jsou použity regulární výrazy a porovnání vůči seznamu předdefinovaných řetězců. Výsledky ukazují, že tento způsob lze použít pro detekci některých síťových útoků využívající protokol HTTP. Práci celkově hodnotím jako dobrou (C).

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

V Brně dne: 30. května 2016

.....
podpis