Posudek oponenta diplomové práce

Student: Havlín Jan, Bc.
Téma: Bezpečnost služby Testing Farm (id 25105)
Oponent: Malinka Kamil, Mgr., Ph.D., UITS FIT VUT

1. **Náročnost zadání** — **průměrně obtížné zadání**
   Jedná se o implementační DP s jasně ohraničeným rámcem. Obtížnost je navýšena integrací do provozního prostředí.
2. **Splnění požadavků zadání** — **zadání splněno**
   Student splnil všechny body zadání na velmi dobré úrovni.
3. **Rozsah technické zprávy** — **je v obvyklém rozmezí**
   Rozsah technické zprávy odpovídá požadavkům na diplomovou práci.
4. **Prezentační úroveň předložené práce** — **85 b. (B)**
   Logická struktura práce je na dobré úrovni. Autor rozumným způsobem představuje řešenou problematiku a technologie potřebné k porozumění větších detailů, i když občas není návaznost jednotlivých částí zřejmá. Kapitola 3 je spíše souhrn generických bezpečnostních problémů bez bližšího zohlednění řešené problematiky. Např. začlenění OWASP neodpovídá testovacím případům.
   Naopak velmi pozitivně hodnotím provedenou analýzu rizik a specifikaci požadavků na řešení. Pro lepší orientaci v popisu implementace by bylo vhodné začlenit vybraná schémata.
5. **Formální úprava technické zprávy** — **90 b. (A)**
   Jazyková a stylistická stránka práce i úroveň typografie je na výborné úrovni.
6. **Práce s literaturou** — **85 b. (B)**
   Odkazované zdroje jsou relevantní tématu a vhodně vybrány.
7. **Realizační výstup** — **75 b. (C)**
   Realizační výstup je funkční a je již nasazen v produkčním prostředí. Ačkoliv jsou sondy poměrně jednoduché, náročnost zvyšuje potřeba vše zasadit do komplexního prostředí Testing Farm a reportovacích nástrojů. O to více překvapuje absence komentářů v kódu. Řešení aktuálně stále obsahuje mnoho false positives. Je otázkou jakým způsobem bude zajištěna analýza komplexních událostí.
8. **Využitelnost výsledků**
   Výsledky jsou již nasazeny v produkčním prostředí a je v plánu je dále rozšiřovat.
9. **Otázky k obhajobě**
   1. V modelu útočníka mi chybí situace, kdy se snaží zaútočit na cizí testovací stroj. Může úspěšným útokem něco získat?
   2. Sledujete mnoho jednoduchých akcí, jakým způsobem chcete vyhodnocovat komplexnější situace a útoky?
   3. Proč jste se rozhodli implementovat vlastní jednoduché "IDS" a nevyužili jste již existující?
10. **Souhrnné hodnocení** — **75 b. dobře (C)**
    Textová část a analýza bezpečnostního rámec je na velmi dobré úrovni. Implementační výsledky práce jsou spíše průměrné. Nicméně obtížnost je navýšena nutnosti integrace do existujícího prostředí a reálným nasazením do produkce. Diskutabilní jsou některá návrhová rozhodnutí, která ovšem byla probrána s konzultantem.

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

V Brně dne: 1. června 2022

Malinka Kamil, Mgr., Ph.D.
oponent